El Modelo de Neutralización de Incentivo Delictivo (MNID) transforma la seguridad tradicional al atacar la raíz del problema: el beneficio esperado del delito. A través de desvalorización funcional y comercial, trazabilidad avanzada, disuasión estratégica y sustitución de motivaciones estructurales, el MNID convierte los activos en objetivos poco atractivos y reduce sistemáticamente la probabilidad delictiva.

Modelo de Neutralización de Incentivo Delictivo

“Desmaterializar el valor”

Autor: Lic. Mauricio Alan Illera Díaz / ORCID ID: 0009-0001-1505-4170 / Researcher ID: OSI-4768-2025 / ID del autor: 9514252 / ID Científico: 2A1E-218D-9A52

Temario:

1. PRESENTACIÓN DEL MANUAL

1.1 Propósito del documento
1.2 Alcance de aplicación
1.3 Sectores objetivo
1.4 Marco conceptual resumido del MNID
1.5 Diferenciación frente a modelos tradicionales de seguridad
1.6 Definiciones operativas clave

2. FUNDAMENTOS ESTRATÉGICOS DEL MNID

2.1 El delito patrimonial como actividad económica informal
2.2 Ecuación del incentivo delictivo
2.3 Teoría de elección racional aplicada a seguridad corporativa
2.4 Mercado negro y cadena de monetización
2.5 Psicología del beneficio percibido
2.6 Riesgo vs. rentabilidad delictiva
2.7 Principios rectores del MNID

3. DIAGNÓSTICO DEL INCENTIVO DELICTIVO

3.1 Identificación de activos críticos
3.2 Análisis de valor real vs. valor en mercado informal
3.3 Mapeo de vulnerabilidades
3.4 Identificación de perfiles de amenaza
3.5 Análisis de cadena de monetización
3.6 Determinación del nivel de atractivo del activo
3.7 Matriz de incentivo delictivo (formato operativo)
3.8 Indicadores base (línea inicial)

4. COMPONENTE I – DESVALORIZACIÓN FUNCIONAL

4.1 Principios de inutilización estratégica
4.2 Separación entre posesión y funcionalidad
4.3 Tecnologías habilitadoras
4.4 Bloqueo remoto y dependencia de servidor
4.5 Diseño anti-extracción y modularidad protegida
4.6 Protocolos de activación controlada
4.7 Pruebas de resistencia funcional
4.8 Indicadores de efectividad
4.9 Checklist de implementación

5. COMPONENTE II – DESVALORIZACIÓN COMERCIAL

5.1 Dinámica del mercado secundario
5.2 Estrategias de reducción de valor de reventa
5.3 Marcaje permanente y serialización

5.4 Microdotting y tecnologías de identificación
5.5 Registro público de propiedad
5.6 Integración con autoridades y plataformas de verificación
5.7 Estrategia contra receptación
5.8 Indicadores de impacto comercial
5.9 Checklist de implementación

6. COMPONENTE III – INCREMENTO DE TRAZABILIDAD

6.1 Niveles de trazabilidad (física, digital, transaccional)
6.2 Arquitectura de rastreo de activos
6.3 Sistemas IoT aplicados a seguridad patrimonial
6.4 Registro inalterable y auditoría automatizada
6.5 Integración con sistemas ERP y control interno
6.6 Gestión de alertas
6.7 Protocolos de recuperación
6.8 Indicadores de trazabilidad efectiva
6.9 Checklist de implementación

7. COMPONENTE IV – DISUASIÓN COMUNICACIONAL

7.1 Psicología de la disuasión
7.2 Diseño de mensajes estratégicos
7.3 Señalización efectiva en puntos críticos
7.4 Comunicación interna y externa
7.5 Transparencia tecnológica como herramienta preventiva
7.6 Gestión de reputación disuasiva
7.7 Medición de percepción de riesgo
7.8 Indicadores de impacto conductual
7.9 Checklist de implementación

8. COMPONENTE V – SUSTITUCIÓN DEL INCENTIVO

8.1 Identificación de motivaciones estructurales
8.2 Análisis socioeconómico del entorno
8.3 Estrategias de reducción de presión económica
8.4 Programas de recompra o regularización
8.5 Integración comunitaria y responsabilidad social
8.6 Modelos de acceso formal alternativo
8.7 Prevención de desplazamiento del delito
8.8 Indicadores de reducción estructural
8.9 Checklist de implementación

9. INTEGRACIÓN SISTÉMICA DEL MNID

9.1 Modelo de implementación por fases
9.2 Sincronización de los cinco componentes
9.3 Gestión del cambio organizacional

9.4 Gobernanza del modelo
9.5 Roles y responsabilidades
9.6 Integración con ISO 31000 y gestión de riesgos
9.7 Integración con compliance y auditoría
9.8 Plan maestro de despliegue

10. MATRICES Y HERRAMIENTAS OPERATIVAS

10.1 Matriz de Incentivo Delictivo (MID)
10.2 Matriz de Cadena de Monetización
10.3 Matriz de Neutralización Progresiva
10.4 Evaluación costo–beneficio del MNID
10.5 Modelo de priorización de activos
10.6 Dashboard de indicadores
10.7 Formatos de auditoría MNID

11. INDICADORES Y MEDICIÓN DE IMPACTO

11.1 KPI estratégicos
11.2 KPI operativos
11.3 Reducción de tasa de intento
11.4 Reducción de éxito delictivo
11.5 Tiempo de monetización ilegal
11.6 Variación en valor de mercado negro
11.7 Análisis comparativo pre y post implementación
11.8 Reportes ejecutivos

12. GESTIÓN DE RIESGOS Y ADAPTACIÓN CRIMINAL

12.1 Posible desplazamiento del delito
12.2 Adaptación tecnológica criminal
12.3 Ataques contra sistemas de bloqueo
12.4 Escenarios de sabotaje interno
12.5 Estrategias de actualización continua
12.6 Simulación de escenarios adversos

13. CASOS DE APLICACIÓN SECTORIAL

13.1 Retail
13.2 Logística y transporte
13.3 Tecnología y electrónicos
13.4 Energía e infraestructura crítica
13.5 Sector farmacéutico
13.6 Sector automotriz
13.7 Activos digitales

14. PROTOCOLO DE AUDITORÍA MNID

14.1 Evaluación inicial
14.2 Verificación de cumplimiento por componente
14.3 Escala de madurez MNID
14.4 Certificación interna
14.5 Plan de mejora continua

15. CONCLUSIONES ESTRATÉGICAS

15.1 Transformación del enfoque de seguridad
15.2 Neutralización vs confrontación
15.3 Impacto sistémico a mediano y largo plazo
15.4 Recomendaciones para expansión sectorial

1. PRESENTACIÓN DEL MANUAL

1.1 Propósito del documento

Este manual tiene como propósito proporcionar una guía operativa, sistemática y técnica para implementar el Modelo de Neutralización de Incentivo Delictivo (MNID) en organizaciones y entornos operativos. Está diseñado para transformar el enfoque tradicional de seguridad y prevención de pérdidas hacia uno que:

1. **Neutraliza el valor** percibido de los bienes objetivo del delito.
2. **Reduce la rentabilidad** del acto delictivo.
3. **Erosiona la motivación** estructural que impulsa el comportamiento delictivo económico.

El objetivo final es lograr una disminución demostrable y sostenida de intentos y éxitos delictivos mediante la intervención directa en la ecuación de costo–beneficio que usan los potenciales infractores en su proceso de toma de decisiones.

Este documento no sólo describe el modelo, sino que establece procedimientos, herramientas, métricas e indicadores de gestión para su aplicación en contextos reales.

1.2 Alcance de aplicación

El alcance de este manual abarca:

- **Organizaciones privadas y corporativas** de cualquier tamaño (PYMES, medianas y grandes).
- **Industrias con activos susceptibles a pérdida patrimonial**, incluyendo inventario, tecnología, vehículos, infraestructura crítica y bienes de alto valor.
- **Entornos logísticos y de transporte** donde el riesgo de robo, extravío o malversación de bienes es alto.
- **Programas de seguridad institucional y centros de decisión sectoriales**, que requieran una metodología estratégica de prevención estructural.
- **Procesos de certificación interna y auditoría de seguridad**, donde se busca medir y demostrar reducción de riesgos de manera cuantitativa.

Este manual no está limitado a un solo tipo de delito, sino que ofrece un enfoque generalizable siempre que se trate de conductas delictivas con componente económico explicable por incentivos.

1.3 Sectores objetivo

Si bien el MNID es conceptual y aplicable a múltiples sectores, su efectividad operacional aumenta en contextos donde los delitos son motivados por la percepción de un beneficio económico o funcional. Entre los sectores en los que este manual se aplica de forma prioritaria se encuentran:

- **Retail y comercio de bienes físicos**, dada la alta incidencia de robo de mercancías y pérdidas por hurtos.
- **Tecnología y electrónica**, donde los bienes tienen alta reventa en mercado informal.
- **Logística y transporte de carga**, especialmente en rutas y centros de distribución con alta tasa de incidencia delictiva.
- **Sector farmacéutico y bienes regulados**, donde el mercado ilegal es activo y lucrativo.
- **Infraestructura crítica**, donde la interrupción de operaciones tiene efectos económicos y sociales de alto impacto.

Además, este manual puede adaptarse a otros sectores mediante módulos sectoriales complementarios.

1.4 Marco conceptual resumido del MNID

El Modelo de Neutralización de Incentivo Delictivo (MNID) parte de una premisa fundamental:

Para que un delito patrimonial ocurra, no basta con la oportunidad; debe existir un beneficio económico o funcional percibido como mayor que los costos y riesgos asociados.

Este enfoque se inspira en la teoría de elección racional, que entiende que los actos delictivos particularmente los contra la propiedad son decisiones en las que el potencial infractor pondera beneficios, costos y probabilidad de detección o captura antes de actuar.

La diferencia clave del MNID es que no busca solamente aumentar barreras o castigos, sino atacar directamente la rentabilidad percibida del acto delictivo, interviniendo en el punto de decisión del actor mediante la reducción del valor funcional y comercial del objeto sustraído.

El modelo opera a través de cinco componentes integrados:

1. **Desvalorización funcional** – eliminar la utilidad del bien una vez separado de su entorno legítimo.
2. **Desvalorización comercial** – reducir la posibilidad de monetización en mercados informales.
3. **Incremento de trazabilidad** – elevar la probabilidad percibida de rastreo y recuperación.
4. **Disuasión comunicacional** – hacer visible que el bien carece de valor para quien lo sustrae.
5. **Sustitución del incentivo** – intervenir en factores estructurales que motivan el delito.

Estos componentes trabajan de forma conjunta para transformar la ecuación motivacional del delito y convertir la comisión del acto en una decisión económicamente desfavorable.

1.5 Diferenciación frente a modelos tradicionales de seguridad

Los modelos tradicionales de seguridad patrimonial y prevención del delito se suelen concentrar en:

- **Incrementar vigilancia física** (guardias, cámaras, barreras).
- **Aumentar severidad de sanciones**.
- **Fortalecer control operativo reactivo**.

Estos enfoques, sin duda, reducen las vulnerabilidades, pero no modifican la motivación delictiva ni integran la dimensión del incentivo económico o funcional.

En criminología tradicional se encuentran modelos como:

- Modelo clásico/neoclásico centrado en la disuasión basada en pena.
- Prevención situacional centrada en oportunidades.
- CPTED: prevención basada en diseño ambiental.

Estas teorías comparten la idea de que modificar el entorno reduce las oportunidades del delito, pero no siempre atacan el factor incentivo económico, que es el combustible central del delito patrimonial.

El MNID, en cambio, posiciona el incentivo como elemento estructural clave, y propone una intervención sistémica que afecta directamente la lógica de rentabilidad del delito, no sólo su ocurrencia momentánea.

1.6 Definiciones operativas clave

A continuación se incluyen términos esenciales para asegurar una interpretación uniforme a lo largo del manual:

- **Delito patrimonial**: conducta ilícita que busca obtener un beneficio económico mediante la sustracción, uso o disposición de bienes de valor.
- **Incentivo delictivo**: beneficio económico o funcional percibido por un potencial infractor que hace atractiva la comisión de un acto delictivo.
- **Valor funcional**: utilidad operativa real de un bien para el infractor después de la sustracción.
- **Valor comercial**: precio que puede obtenerse por la venta del bien en mercados formales o informales.
- **Neutralización del incentivo**: proceso de reducción o eliminación de la utilidad y valor de un bien para desincentivar su sustracción.

Estas definiciones establecerán la base conceptual y operativa para los procedimientos y métricas desarrolladas en los capítulos subsiguientes.

2 FUNDAMENTOS ESTRATÉGICOS DEL MNID

2.1 El delito patrimonial como actividad económica informal

El delito patrimonial (como el robo, hurto, receptación, fraude y otras formas de sustracción de bienes) tiene una dimensión económica clara: los bienes robados se intercambian, convierten, venden o utilizan para obtener beneficios posteriores. En este sentido, muchos actos delictivos no son conductas aisladas de destrucción o daño social,

sino actividades que operan dentro de una economía paralela o informal, con oferta, demanda, precios y canales de comercialización propios.

Características económicas del delito patrimonial

- **Producen bienes susceptibles de intercambio:** los bienes robados son convertibles en dinero u otros beneficios.
- **Generan mercados secundarios:** lugares donde se comercializa lo robado (mercado negro, talleres informales, intermediarios, “compraventas”).
- **Reducen costos al eliminar formalidades:** no pagan impuestos ni regulaciones, y evaden controles institucionales típicos de mercados legales.

Una característica clave observada por criminólogos y economistas del delito es que los mercados de bienes robados reducen el costo transaccional para el infractor, facilitando su reinserción en otro bien o en dinero líquido sin pasar por canales formales. Esto convierte al delito patrimonial en una actividad que responde a incentivos económicos concretos, no solo a impulsos antisociales.

2.2 Ecuación del incentivo delictivo

Una de las bases conceptuales del MNID es que el delito patrimonial es una decisión motivada por incentivos: el potencial infractor pondera posibles ventajas frente a los costos de actuar. Este proceso se resume en una fórmula similar a la usada en economía clásica:

Delito ocurre si:
Beneficio percibido > (Costo + Riesgo percibido)

Componentes de la ecuación

- **Beneficio percibido:** ganancia económica o funcional que se espera obtener (dinero, reventa, utilidad del bien).
- **Costo:** esfuerzo físico, tiempo invertido, recursos necesarios.
- **Riesgo percibido:** probabilidad de ser detectado, detenido o castigado.

Cuando el beneficio percibido es suficientemente alto en comparación con los costos y el riesgo, la probabilidad de que ocurra un delito patrimonial aumenta. Esta lógica es central tanto en la teoría de elección racional, como en modelos económicos del delito.

2.3 Teoría de elección racional aplicada a seguridad corporativa

La Teoría de Elección Racional postula que muchas personas cometen delitos después de valorar mentalmente los beneficios esperados frente a los riesgos y costos asociados. No se trata de mera impulsividad, sino de una decisión racional informada por incentivos percibidos y condiciones del entorno.

Implicaciones operativas

En seguridad corporativa, esta teoría sugiere que la prevención del delito no solo debe aumentar riesgos o barreras, sino modificar la percepción de beneficios:

- Reducir los beneficios percibidos (menor valor del botín).
- Aumentar la percepción de riesgo o de inutilidad del objeto robado.
- Hacer visible que el beneficio no será realizable.

La teoría también reconoce que, a veces, la racionalidad del infractor está limitada por falta de información o sesgos cognitivos, pero el modelo aún proporciona una estructura robusta para diseñar estrategias de prevención.

2.4 Mercado negro y cadena de monetización

El mercado negro refiere a un sistema económico informal donde bienes y servicios se compran y venden fuera de los canales legales. En el contexto del delito patrimonial, estos mercados sirven como la vía de monetización para bienes robados, al reducir costos transaccionales (p. ej., sin facturas, impuestos ni verificación formal) y al ofrecer un espacio donde el infractor puede convertir lo robado en dinero o bienes útiles.

Roles del mercado negro en la incentivación

- **Canal de reventa:** transforma bienes robados en dinero.
- **Reducción del costo de entrada:** los intermediarios facilitan la venta sin controles legales estrictos.
- **Demanda persistente:** hay clientes dispuestos a comprar bienes más baratos, aunque sean ilícitos.

Las investigaciones muestran que cuando estos mercados son más regulados o controlados (por ejemplo, con verificación de origen de bienes o supervisión de “chatarra” y talleres), la incidencia de delitos patrimoniales puede disminuir porque se eleva el riesgo y se reduce la posibilidad de monetización inmediata.

2.5 Psicología del beneficio percibido

Más allá de un cálculo económico, la decisión delictiva también tiene un componente psicológico profundo: el infractor evalúa no solo el beneficio real, sino el beneficio percibido, que puede estar influenciado por:

- Experiencias previas de éxito o fracaso.
- Normas sociales en su entorno.
- Información disponible sobre la probabilidad de ser capturado.
- Percepción del valor económico y funcional del bien.

La psicología del delito demuestra que la percepción puede ser tan o más determinante que la realidad objetiva: si un delincuente percibe que un bien tiene poco valor o que su

beneficio real es marginal, su motivación disminuye, incluso si en realidad podría generar ganancia.

2.6 Riesgo vs. rentabilidad delictiva

La relación entre el riesgo percibido y la rentabilidad esperada en la actividad delictiva es similar al concepto de trade-off en economía: se busca un balance entre el beneficio potencial y el riesgo que se asume. Un delito resulta atractivo solo si la expectativa de ganancia supera los riesgos involucrados, como la posibilidad de ser detenido, el castigo legal, o el esfuerzo requerido. Es decir, el delincuente evalúa si vale la pena arriesgarse en función de lo que puede obtener y lo que puede perder.

Factores que impactan esta relación

- **Probabilidad de captura:** Mientras más alta sea la posibilidad de ser arrestado, menor resulta la rentabilidad del acto delictivo.
- **Severidad del castigo:** Castigos más estrictos reducen el atractivo de cometer delitos, disminuyendo la ganancia esperada.
- **Facilidad de mercado secundario:** Si no hay canales seguros para vender o monetizar lo robado, la rentabilidad baja considerablemente.

Así, un bien puede parecer atractivo por su valor económico, pero si el riesgo es elevado o las posibilidades de convertirlo en dinero son reducidas, la motivación para cometer el delito disminuye notablemente.

2.7 Principios rectores del MNID

Para asegurar la efectividad y coherencia del MNID, se establecen siete principios estratégicos que guían tanto su diseño como su implementación:

1. Neutralización del incentivo económico

La finalidad no es hacer imposible el delito, sino lograr que sea económicamente poco atractivo, modificando la ecuación de costo-beneficio desde la percepción del delincuente.

2. Reducción del mercado secundario

Se busca intervenir, directa o indirectamente, en los canales que permiten la venta de bienes robados, disminuyendo su atractivo y la posibilidad de convertirlos en dinero.

3. Integración de percepción y realidad

Es fundamental actuar tanto sobre la realidad objetiva (por ejemplo, bloqueos funcionales, trazabilidad) como sobre la percepción subjetiva (mediante campañas de comunicación disuasiva) para influir en la toma de decisiones del delincuente.

4. Intervención en múltiples fases del delito

Es necesario intervenir no solo durante la comisión del delito, sino también en todas las etapas posteriores (como la venta, transporte y reventa), para disminuir la rentabilidad total y dificultar la cadena criminal.

5. Sustitución estructural de motivaciones

Es importante abordar los factores estructurales que impulsan la comisión de delitos, como la necesidad económica o la falta de oportunidades, y fortalecer alternativas legítimas que desmotiven la actividad ilícita.

6. Medición y ajuste continuo

Se deben implementar indicadores cuantitativos y cualitativos para conocer la evolución de la ecuación delictiva en el tiempo y ajustar las estrategias según los resultados obtenidos.

7. Integración con políticas de seguridad sistémicas

El MNID no sustituye los sistemas de seguridad convencionales, sino que los complementa y fortalece, especialmente en situaciones donde los incentivos económicos para delinquir son elevados.

3. DIAGNÓSTICO DEL INCENTIVO DELICTIVO

El diagnóstico del incentivo delictivo es el proceso fundamental para entender por qué, qué y cómo ciertos bienes o activos se convierten en objetivos de conducta delictiva. Este diagnóstico no sólo determina la probabilidad de ocurrencia de hechos delictivos, sino que evalúa el atractivo del objetivo desde la perspectiva del infractor, abarcando valor económico, funcional y percepciones subjetivas que influyen en la decisión delictiva.

Este capítulo detalla todas las fases necesarias para llevar a cabo un diagnóstico riguroso, desde identificar los activos críticos hasta construir una matriz de incentivo delictivo cuantificable.

3.1 Identificación de activos críticos

La identificación de activos críticos es el paso inicial y más importante en cualquier análisis de riesgo o prevención del delito. Un activo crítico es aquello cuya pérdida o sustracción causaría un impacto significativo en la operación, continuidad del negocio o valor económico para la organización.

La identificación debe incluir no solo bienes físicos, sino también:

- **Activos tangibles:** inventarios, equipos, infraestructura, vehículos.
- **Activos intangibles:** propiedad intelectual, bases de datos, reputación.
- **Activos operativos alternativos:** licencias de software, credenciales y acceso.
- **Activos humanos:** personal clave cuya ausencia o daño impacte operaciones.

La metodología empieza por catalogar los activos y determinar cuáles tienen un valor económico significativo o una importancia crítica para la operación. Esto se hace mediante entrevistas con áreas clave, revisión de estados financieros, procesos operativos y análisis de dependencias funcionales internas.

3.2 Análisis de valor real vs. valor en mercado informal

Una vez identificados los activos críticos, es indispensable evaluar dos valores diferentes pero complementarios:

a) Valor real

Este valor corresponde al costo de reemplazo, pérdida de operación, impacto financiero y reputación si el activo se pierde o es dañado dentro del sistema formal. Incluye:

- Valor de reposición
- Pérdida de ingresos
- Costos de interrupción operativa
- Costos reputacionales

Este valor suele medirse en términos financieros y gerenciales.

b) Valor en mercado informal

Aquí se evalúa cuánto puede valer ese mismo activo si se vende en el mercado ilegal, secundario o de bienes robados. Esta evaluación considera:

- Precio promedio pagado por intermediarios del mercado negro
- Demanda en canales informales (compraventa, despiece)
- Facilidad de reventa
- Tiempo que tarda el activo en monetizarse fuera de los canales formales

La literatura sobre reducción del mercado delictivo señala que la existencia de canales de venta de bienes robados (mercado negro) es un factor clave en la incentivación del delito: cuanto más fácil es la reventa, mayor es el incentivo para robar.

3.3 Mapeo de vulnerabilidades

El mapeo de vulnerabilidades se refiere a identificar las debilidades que pueden ser explotadas para que el delito ocurra o para que el bien pierda su valor funcional o sea mal utilizado.

Este mapeo incluye:

- **Vulnerabilidades físicas:** accesos no controlados, almacenamiento inseguro, logística deficiente.

- **Vulnerabilidades tecnológicas:** falta de cifrado de datos, dispositivos sin protección, sistemas sin controles.
- **Vulnerabilidades humanas:** falta de capacitación, procesos inadecuados, errores operativos.
- **Vulnerabilidades contractuales o de proceso:** proveedores no auditados, terceros sin controles.

En el contexto de MNID, las vulnerabilidades no sólo importan por sí mismas, sino por cómo impactan la facilidad con la que un delincuente puede transformar un activo en beneficio (real o percibido). El objetivo es detectar puntos donde la neutralización del incentivo puede ser más efectiva.

3.4 Identificación de perfiles de amenaza

La identificación de perfiles de amenaza implica caracterizar quiénes son los posibles agentes delictivos, su modus operandi y sus objetivos. Esto permite anticipar no sólo qué activos están en riesgo, sino cómo podrían atacarlos.

Los perfiles de amenaza pueden incluir:

Delincuencia común

- Oportunista, busca activos de fácil acceso y de rápida monetización.

Crimen organizado

- Redes estructuradas con canales establecidos para monetizar bienes robados.

Empleados internos

- Personas con acceso privilegiado que pueden facilitar sustracciones internas.

Cada perfil tiene características distintas de riesgo y afecta la forma en que se prioriza la neutralización del incentivo.

La creación de perfiles también debe considerar variables como:

- Historia de incidentes previos
- Información de inteligencia pública o privada
- Factores socioeconómicos locales y regionales

Este enfoque de amenazas permite pasar de una visión estática de riesgo a una más dinámica y prospectiva.

3.5 Análisis de cadena de monetización

La cadena de monetización es el proceso completo que sigue un bien desde el momento en que es sustraído hasta que es convertido en dinero, uso o reventa.

Identificar esta cadena es vital, pues cada eslabón puede:

- Reducir el valor real del activo (neutralización funcional)
- Interrumpir la monetización (bloqueo de mercado)
- Aumentar el riesgo percibido para el delincuente

Un análisis completo de la cadena incluye:

1. **Sustracción:** cómo y dónde se toma el bien.
2. **Movilidad/internamiento:** forma en que se retira fuera del entorno original.
3. **Canales secundarios:** intermediarios, mercado negro, talleres de despiece.
4. **Conversión final:** venta, reventa o uso propio.

El enfoque de reducción del mercado (Market Reduction Approach) respalda la idea de que interrumpir el mercado ilegal de bienes sustraídos disminuye la incidencia del delito.

3.6 Determinación del nivel de atractivo del activo

Con la información anterior se construye un índice o puntuación de atractivo del activo para un potencial infractor. Este índice combina:

- Valor en mercado informal
- Facilidad de sustracción (basado en vulnerabilidades)
- Riesgo de detección y captura
- Percepción de utilidad tras la sustracción

Un activo con alto atractivo puede tener, por ejemplo:

- Alto valor de reventa
- Fácil acceso o baja protección
- Alta demanda en mercado negro
- Bajo riesgo percibido por delincuentes

La determinación de este nivel debe cuantificarse para facilitar su comparación con otros activos. Esto permite priorizar esfuerzos de neutralización del incentivo.

3.7 Matriz de incentivo delictivo (formato operativo)

La Matriz de Incentivo Delictivo es una herramienta práctica que cruza variables clave para determinar el nivel de riesgo y atractivo de un activo.

Ejemplo de estructura:

Activo	Valor real	Valor mercado informal	Vulnerabilidades (1-5)	Amenaza (1-5)	Monetización fácil (1-5)	Índice de atractivo
Activo A	Alto	Medio	4	3	5	X
Activo B	Medio	Alto	2	4	2	Y

Cada variable puede ponderarse según el contexto de la organización.

Esta matriz permite:

- Visualizar cuál es el activo prioritario
- Identificar canales críticos a intervenir
- Establecer métricas comparativas entre distintos activos

3.8 Indicadores base (línea inicial)

Establecer indicadores de línea base es esencial para medir la efectividad de las medidas de neutralización del incentivo. Algunos indicadores iniciales incluyen:

1. Tasa de intentos de sustracción por activo
2. Tasa de éxito de sustracción
3. Tiempo promedio de monetización fuera del sistema
4. Variación del valor de mercado informal antes y después de intervenciones
5. Número de incidentes por perfil de amenaza

Estos indicadores permiten medir tanto la eficacia de controles como la disminución de atractivo del activo tras implementar el modelo.

4. COMPONENTE I – DESVALORIZACIÓN FUNCIONAL

El objetivo del componente de Desvalorización Funcional es hacer que un activo pierda utilidad práctica real para el infractor una vez que ha sido separado de su entorno legítimo. En el contexto del MNID, esto significa que incluso si un bien es sustraído, su valor como botín se reduce o elimina porque no puede cumplir su función normal, no puede ser utilizado, ni convertido en beneficio sin intervención autorizada. Este enfoque ataca directamente el incentivo económico y funcional del delito.

4.1 Principios de inutilización estratégica

La desvalorización funcional no se trata de destruir un activo de forma indiscriminada, sino de alterarlo de manera que pierda su funcionalidad fuera de un entorno controlado sin afectar su valor cuando se usa legítimamente.

Fundamentos

La inutilización estratégica debe ser:

- **Selectiva:** afecta la funcionalidad del activo solo fuera del entorno seguro.
- **Reversible o controlada:** permite habilitar el activo por medio legítimo si es recuperado.
- **Transparente:** el usuario legítimo debe saber cómo funciona y cómo recuperarlo con seguridad.

Esto se logra a través de mecanismos que dependen de sistemas de control central, comunicación segura o limitaciones de operación cuando no se cumplen ciertas condiciones (p. ej., ausencia de credenciales, fuera de ubicación geográfica autorizada). El principio básico es que tener el bien no necesariamente equivale a poder usarlo.

4.2 Separación entre posesión y funcionalidad

Una pieza clave de la desvalorización funcional es distinguir claramente entre:

- **Posesión física:** cuando el infractor físicamente tiene el bien.
- **Funcionalidad operativa:** la capacidad de usarlo para el propósito para el cual fue diseñado.

Por ejemplo:

✅ *Robar un celular* → posesión física.
❌ *No poder encenderlo o usarlo* → funcionalidad bloqueada (porque necesita autenticación o conexión a servidor para operar).

Esta separación reduce el valor del botín en el mercado informal y disuade actos delictivos porque la recompensa esperada se vuelve incierta o nula.

4.3 Tecnologías habilitadoras

Para hacer posible la desvalorización funcional se recurre a diversas tecnologías modernas que integran capacidades de control, comunicación y bloqueo:

Tecnologías principales

1. **Kill Switch / "Kill Pill":** mecanismo que permite desactivar remotamente un dispositivo o sistema completo, dejándolo funcionalmente inútil sin la autorización adecuada.
2. **Inmovilizadores electrónicos (immobilisers):** sistemas que impiden que un motor o mecanismo arranque a menos que se detecte la credencial autorizada.

3. **Telemática y GPS con capacidades de bloqueo remoto:** permiten ubicar el activo y desactivarlo cuando se detecta uso no autorizado.
4. **Plataformas de control centralizado:** servidores o servicios de backend que validan credenciales y autorizaciones antes de permitir la operación real del activo.
5. **Sistemas IoT con reglas geográficas o temporales:** activan o desactivan funciones según ubicación o zonas permitidas (geofencing).

Estas tecnologías integradas forman la base técnica para que un activo continúe existiendo físicamente pero pierda su utilidad práctica para el infractor.

4.4 Bloqueo remoto y dependencia de servidor

Una de las técnicas más efectivas de desvalorización funcional es el bloqueo remoto mediante un sistema central, que puede:

- Desactivar funciones clave del dispositivo o maquinara.
- Requerir autenticación desde un servidor antes de habilitar su uso.
- Operar reglas específicas como geocercas o ventanas de tiempo autorizadas.

Cómo funciona

1. **Componente en el activo:** hardware o firmware que solo permite operación si recibe una autorización válida del servidor central.
2. **Servidor de control:** verifica la solicitud con credenciales, condiciones de seguridad y reglas definidas.
3. **Señal de autorización:** si todo es legítimo, el servidor permite la operación. Si no, el activo permanece inactivo o funcionalmente limitado.

Este método es común en sistemas modernos de gestión de flotas, vehículos conectados, equipos industriales y dispositivos IoT avanzados y puede ser aplicado también en activos corporativos críticos para neutralizar su valor para un delincuente.

4.5 Diseño anti-extracción y modularidad protegida

El diseño físico del activo también puede contribuir a la desvalorización funcional:

Estrategias de diseño

- **Módulos inseparables sin herramientas especiales:** dificultan su extracción o reutilización fuera del sistema.
- **Sellos o etiquetas de seguridad inteligentes:** que alertan o bloquean funcionalidad si se manipulan sin autorización.
- **Integración de circuitos de bloqueo en elementos esenciales del activo:** para que la extracción o intervención rompa circuitos de autenticación o detección.

Estas técnicas refuerzan la idea de que el activo no es inmediatamente utilizable aunque esté físicamente presente. El diseño anti-extracción complica que un infractor pueda extraer partes útiles sin invalidar la funcionalidad del bien completo.

4.6 Protocolos de activación controlada

Un elemento crítico para hacer funcionar la desvalorización funcional es la definición de protocolos de activación controlada, que determinan cuándo y cómo el activo puede habilitar su funcionalidad:

Componentes del protocolo

1. **Verificación de identidad:** autenticación del usuario legítimo mediante credenciales confiables.
2. **Condiciones ambientales o de contexto:** por ejemplo, estar en ubicación geográfica autorizada, cumplir horarios, detectar sensores internos seguros.
3. **Canal seguro de comunicación:** para que la señal de habilitación no pueda ser interceptada o suplantada.
4. **Reglas de reactivación tras recuperación del activo:** procedimientos de restablecimiento luego de robo o pérdida.

Estos protocolos hacen que la llegada física al bien no sea suficiente para poder usarlo, reduciendo de manera significativa su atractivo para el delito.

4.7 Pruebas de resistencia funcional

Una vez implementados mecanismos de desvalorización funcional, es indispensable realizar pruebas de resistencia funcional, es decir:

- Evaluar si los sistemas de bloqueo o dependencia operan bajo ataques reales o simulados.
- Determinar si la funcionalidad queda efectivamente inutilizada cuando las condiciones de seguridad no se cumplen.
- Evaluar vulnerabilidades como intentos de suplantación de credenciales, bypass de sistemas, o sabotaje físico.

Estas pruebas deben incluir:

- Tests de penetración tecnológica
- Simulaciones de extracción física
- Análisis de fallos de comunicación
- Revisión de protocolos de activación

El objetivo es asegurar que la desvalorización funcional es robusta, difícil de anular por manipulación común.

4.8 Indicadores de efectividad

Para medir si la desvalorización funcional está teniendo un impacto real sobre el incentivo delictivo, deben establecerse indicadores de efectividad, tales como:

Indicadores principales

- Tasa de casos de robo detectados en los que el activo fue inutilizado (es decir, el delincuente no pudo usarlo).
- Tiempo promedio de inutilización después de intento de sustracción.
- Porcentaje de intentos de robo que terminan sin reventa o reutilización del bien.
- Número de fallos de protocolo de activación o bypass detectados durante pruebas.
- Reducción del valor de reventa en mercado informal atribuible a funcionalidades bloqueadas.

Estos indicadores permiten evaluar no sólo que la tecnología está instalada, sino que impacta la ecuación de incentivo del interno.

4.9 Checklist de implementación

Para asegurar que la desvalorización funcional se implementa de forma organizada y consistente, se recomienda la siguiente lista de verificación operativa:

Checklist

- ✓ Identificación clara de activos que se desvalorizarán funcionalmente.
- ✓ Selección de tecnologías habilitadoras apropiadas para cada activo.
- ✓ Diseño e integración de mecanismos de bloqueo remoto o servidor dependiente.
- ✓ Definición de protocolos de activación controlada.
- ✓ Integración física de diseño anti-extracción o modularidad protegida.
- ✓ Pruebas de resistencia funcional en ambiente controlado.
- ✓ Establecimiento de indicadores de efectividad relevantes.
- ✓ Documentación de protocolos y reglas de uso.
- ✓ Capacitación a personal de operación y seguridad.
- ✓ Auditorías periódicas y ajustes según resultados de indicadores.

5. COMPONENTE II — DESVALORIZACIÓN COMERCIAL

La desvalorización comercial es el proceso estratégico mediante el cual se reduce el valor que los bienes robados tienen en el mercado secundario o informal. Este componente busca interrumpir la cadena de monetización que transforma un bien sustraído en dinero o utilidad para el delincuente o intermediario. En otras palabras, no se trata solo de proteger los bienes, sino de hacer que, aunque se roben, su valor de reventa sea mínimo o nulo.

5.1 Dinámica del mercado secundario

El mercado secundario (o mercado de bienes robados) es la red informal donde los activos sustraídos se venden, intercambian o reutilizan. Es una parte fundamental de la economía informal que multiplica la rentabilidad del delito patrimonial porque provee un canal para convertir bienes robados en dinero o bienes útiles.

Cómo opera este mercado

Intermediarios (fences): individuos o negocios que compran bienes robados para luego venderlos a terceros.

Demanda de consumidores: existe una base de compradores dispuestos a adquirir bienes a precio reducido, a veces sin verificar su procedencia.

Canales informales: tianguis, mercados de pulgas, plataformas no reguladas y comercio ilícito offline u online.

Efecto retroalimentador: cuanto más eficiente y amplio es este mercado, mayor es el incentivo para cometer robos porque los delincuentes pueden recuperar rápidamente su inversión ilícita.

Romper o debilitar esta dinámica es clave para que la desvalorización comercial funcione: si el mercado informal no está dispuesto a pagar por bienes robados, el incentivo para robar disminuye.

5.2 Estrategias de reducción de valor de reventa

El valor de reventa puede ser atacado de dos maneras complementarias:

1. Aumentar el riesgo para compradores

Políticas legales que hagan ilegal comprar bienes sin trazabilidad.

Obligación de verificar el origen de los bienes antes de comprar o vender. Esto cambia la ecuación del comprador y hace menos atractivo adquirir bienes presumiblemente robados.

2. Reducir la confianza del mercado

Marcar bienes con identificación única, de modo que no puedan ser revendidos sin revelar su procedencia.

Promover herramientas de verificación pública, donde los compradores puedan comprobar el origen legal de un bien.

3. Educación del consumidor

Campañas para explicar que comprar bienes sin procedencia legal fomenta el delito.

Incentivar que compradores honestos sólo adquieran bienes con documentación adecuada.

Estas estrategias, combinadas, reducen tanto el atractivo del comprador como la facilidad de monetización de bienes robados.

5.3 Marcaje permanente y serialización

El marcaje permanente consiste en aplicar identificadores únicos (números de serie, QR, marcas visibles o invisibles) que permitan rastrear un bien hasta su dueño legítimo.

Beneficios

Disuade a compradores informales, ya que las marcas visibles o rastreables hacen más difícil vender el bien sin levantar sospechas o requerir pruebas de propiedad.

Facilita la recuperación del bien y la identificación del propietario legítimo.

Reduce la posibilidad de que bienes robados se mezclen con bienes legítimos en el mercado.

Ejemplo clásico

La iniciativa Operation Identification en Estados Unidos promueve que los dueños marquen propiedad con identificadores legibles, publiquen números de serie y registren los bienes en bases de datos policiales para disuadir el robo y facilitar recuperación.

5.4 Microdotting y tecnologías de identificación

Más allá de los números de serie visibles, existen tecnologías forenses de identificación como el microdotting y sistemas basados en códigos invisibles o microcódigos sintéticos que permiten una verificación detallada y única del bien.

Qué es microdotting

Consiste en adherir miles de micro-puntos con un código único a los bienes, prácticamente invisibles a simple vista.

Este código se puede leer con herramientas especializadas y vincular el objeto con un registro de propiedad.

A menudo se combina con marcadores sintéticos de ADN o microcódigos forenses para una trazabilidad altamente confiable.

Valor estratégico

Reduce drásticamente la capacidad de los intermediarios de “lavar” bienes robados al foro informal.

Si se detecta un microcódigo registrado, el artículo puede ser confiscado sin que el vendedor pueda reclamar propiedad legítima.

Esto impacta negativamente la confianza del mercado negro en bienes marcados, reduciendo su valor comercial.

5.5 Registro público de propiedad

Un registro público de bienes (equivalente al registro de vehículos robados o bases de datos de propiedad) juega un papel crítico en la desvalorización comercial.

Funciones del registro

Permite verificar la legalidad de un bien antes de la venta.

Sirve como base de datos para que autoridades rastreen bienes robados recuperados.

Permite a compradores legítimos comprobar la procedencia antes de adquirir un objeto de segunda mano.

La ausencia de estos registros facilita el mercado ilegal porque los intermediarios y compradores no tienen forma de verificar origen de un bien. Los sistemas de registro aumentan el costo de vender bienes robados y reducen el valor de reventa.

5.6 Integración con autoridades y plataformas de verificación

Reducir el valor de reventa no funciona sin cooperación institucional. La integración con autoridades y plataformas ciudadanas permite:

Ventajas

Acceso de fuerzas del orden a bases de datos de bienes marcados o registrados.

Capacidad de verificar bienes en tiempo real en tiendas de segunda mano y plataformas online.

Intercambio de información entre plataformas comerciales y autoridades para bloquear ventas sospechosas.

Este enfoque integrado es parte de lo que se conoce como Market Reduction Approach, que busca reducir mercados de bienes robados mediante intervención en la oferta y la demanda del mercado ilegal.

5.7 Estrategia contra receptación

La receptación es el acto de recibir, comprar o comerciar bienes sabiendo (o con sospecha fundada) que son producto de robo. La estrategia contra receptación es crucial porque sostiene gran parte del valor del mercado de bienes robados.

Elementos de una estrategia eficaz

Legislación clara e incentivos para que compradores y vendedores en mercados formales verifiquen origen.

Sanciones para intermediarios y receptadores tanto civiles como penales.

Protocolos anti-reventa obligatorios para tiendas de segunda mano y casas de empeño: verificar antecedentes y registrar transacciones.

Reducir la receptación hace que los bienes robados pierdan su canal de liquidez, lo que disminuye su valor comercial.

5.8 Indicadores de impacto comercial

Las siguientes métricas permiten evaluar si las estrategias de desvalorización comercial realmente están reduciendo el incentivo económico del delito:

Indicadores clave

Reducción en volumen de bienes robados ofertados en mercados informales.

Porcentaje de bienes registrados o marcados recuperados vs. vendidos.

Número de compras rechazadas por falta de verificación de origen.

Tasa de incautación de bienes sospechosos en mercados de segunda mano.

Variación en precios de reventa de bienes previamente robados (antes y después de implementaciones).

Cada uno de estos indicadores refleja cómo el valor de mercado de bienes robados se erosiona con medidas de desvalorización comercial.

5.9 Checklist de implementación

Para una implementación ordenada y eficaz de la desvalorización comercial, utiliza este checklist:

Checklist

- ✓ Identificación de mercados secundarios relevantes para los activos protegidos.
- ✓ Definición de tecnologías de marcaje y serialización apropiadas.
- ✓ Implementación de microdotting u otros sistemas de identificación avanzada.
- ✓ Creación o vinculación con un registro público de propiedad.
- ✓ Integración con autoridades y plataformas transaccionales para verificación de bienes.
- ✓ Establecimiento de protocolos anti-reventa para casas de empeño/segunda mano.
- ✓ Campañas de educación al consumidor sobre riesgos de comprar bienes sin documentación.
- ✓ Monitoreo de indicadores de impacto comercial.
- ✓ Actualización periódica de estrategias según resultados de métricas.

6. COMPONENTE III — INCREMENTO DE TRAZABILIDAD

El incremento de trazabilidad apunta a aumentar la visibilidad, seguimiento y registro continuo de los activos durante todo su ciclo de vida.
Esto significa que cada activo, desde su ingreso en el inventario hasta su salida o uso, esté registrado, localizado y monitoreado en tiempo real, con la capacidad de reconstruir su trayectoria completa. Debido a que la trazabilidad influye directamente en la percepción de riesgo y en la capacidad de recuperarlo, se convierte en una pieza clave para erosionar el incentivo delictivo.

6.1 Niveles de trazabilidad (física, digital, transaccional)

La trazabilidad no es un concepto único, sino que se despliega en tres niveles complementarios:

Trazabilidad física

Se refiere al seguimiento real y tangible de activos usando tecnologías de localización (GPS, RFID, beacons, sensores BLE). El objetivo es conocer dónde está físicamente el activo en cada momento, independientemente de quien lo posea. Esto elimina puntos ciegos en el movimiento de bienes y reduce la posibilidad de pérdida o robo no detectado.

Trazabilidad digital

Consiste en digitalizar toda la información relevante del activo (identificador único, historial de uso, estado técnico, eventos de mantenimiento, historial transaccional). Esto se logra a través de una base de datos centralizada o distribuida que puede ser consultada y auditada en tiempo real.

Trazabilidad transaccional

Representa el registro de todas las acciones, transferencias o eventos asociados a un activo, incluyendo quién lo autorizó, cuándo se movió, qué se hizo con él y si hubo alertas de seguridad. Esto habilita auditorías y reconstrucciones históricas confiables y seguras, incluso cuando un activo cambia de custodia.

6.2 Arquitectura de rastreo de activos

Para implementar trazabilidad efectiva, se necesita una arquitectura tecnológica y procesal integrada que conecte sensores físicos con sistemas centrales de gestión y operaciones. Los componentes principales son:

Identificación del activo

Cada activo recibe un identificador único (RFID, código QR, BLE tag) que sirve como “huella digital” y permite su reconocimiento automático cada vez que pasa por un punto de lectura.

Red de captura de datos

Sensores, lectores, gateways y dispositivos IoT capturan información de ubicación, movimiento y estado del activo en tiempo real o por demanda.

Plataforma centralizada de datos

Todos los eventos son enviados a una base de datos o un sistema de gestión de activos donde se almacena y puede ser consultado para auditorías, análisis y alertas.

Paneles de control y analítica

Dashboards customizables muestran el estado y la ubicación actual de activos, históricos de movimiento, alertas y métricas de desempeño.

Esta arquitectura permite cerrar el ciclo completo de conocimiento del activo, desde su identificación física hasta su registro digital y transaccional continuo.

6.3 Sistemas IoT aplicados a seguridad patrimonial

La adopción del Internet de las Cosas (IoT) para el seguimiento de activos ha revolucionado la trazabilidad, ofreciendo visibilidad en tiempo real y automatización de tareas de rastreo que antes eran manuales y propensas al error.

Tecnologías clave de IoT

- **GPS & geoposicionamiento:** para localizar activos móviles o grandes, como vehículos o maquinarias.
- **RFID y BLE (Bluetooth Low Energy):** para activos dentro de instalaciones, identificación automática sin línea de vista y detección por proximidad.
- **Sensores ambientales:** que monitorean condiciones (temperatura, vibración, humedad) para activos sensibles.
- **Gateways IoT:** que actúan como puentes entre sensores y la red/servidor central.

Beneficios de IoT en seguridad patrimonial

- **Alerta temprana de movimiento no autorizado** (p. ej., agente que cruza un geofence).
- **Mayor probabilidad de recuperación del activo robado** por ubicación en tiempo real.
- **Prevención por disuasión**: los delincuentes saben que están siendo rastreados.

En conjunto, estas tecnologías *no solo rastrean activos, sino que transforman los datos en inteligencia operativa* para seguridad integral.

6.4 Registro inalterable y auditoría automatizada

Un sistema de trazabilidad confiable requiere que todos los datos de seguimiento estén registrados de forma segura, verificable y no modificable sin evidencia de cambio. Esto se logra mediante:

Registro inalterable

Los eventos de trazabilidad (como ubicación, transferencia, acceso) deben guardar un historial íntegro. Esto puede potenciarse con tecnologías como blockchain, que proveen un registro distribuido, resistente a manipulaciones y auditable por múltiples partes interesadas.

Auditoría automatizada

Gracias a la captura de datos automatizada, se pueden generar auditorías periódicas sin intervención manual —lo que elimina errores, posibilita evaluaciones continuas y garantiza cumplimiento regulatorio (p. ej., ISO 55000 para gestión de activos).

Estos registros automatizados son vitales para:

- Detectar brechas o anomalías de movimiento.
- Generar informes de cumplimiento.
- Proveer evidencia sólida en investigaciones internas o judiciales.

6.5 Integración con sistemas ERP y control interno

La trazabilidad no opera aislada, sino conectada con los sistemas centrales de gestión para reforzar el control interno corporativo.

Integración con ERP (Enterprise Resource Planning)

Los sistemas de seguimiento de activos pueden sincronizar información con:

- ERP para actualizar inventarios en tiempo real.
- Sistemas de mantenimiento (CMMS).
- Bases de datos contables y de auditoría.

Esto permite que cualquier cambio físico detectado (como un movimiento de activo sin autorización) se refleje inmediatamente en el registro contable o en el flujo de procesos internos, reduciendo errores y posibles brechas de control.

Integración con control interno

Esto implica establecer conexiones con:

- Procedimientos de inventario físico periódico.
- Alertas automáticas asociadas a roles y responsabilidades de custodia.
- Sistemas de autorización y roles de acceso.

La integración refuerza la consistencia entre lo que “debería ocurrir” (procesos internos) y “lo que realmente ocurre” (datos de trazabilidad).

6.6 Gestión de alertas

Las alertas son un pilar operativo del monitoreo de activos. Un sistema de trazabilidad eficiente debe permitir:

Tipos de alertas

- **Geocercas:** notificaciones automáticas cuando un activo entra o sale de zonas definidas.
- **Movimientos fuera de hora autorizada.**
- **Anomalías de estado** (p. ej., vibraciones inusuales que pueden indicar manipulación).
- **Pérdida de señal o desconexión sospechosa.**

Canales de notificación

- Paneles de control de gestión.
- Mensajes a supervisores o seguridad (correo, SMS, app).
- Integración con sistemas de respuesta (vigilancia o autoridades).

Una buena gestión de alertas transforma datos de movimiento en acciones preventivas y reactivas, mejorando la probabilidad de intervenir antes de que la pérdida se consolide.

6.7 Protocolos de recuperación

La trazabilidad no solo debe permitir conocer dónde está un activo, sino también definir pasos claros de acción cuando ocurre un evento adverso, como:

1. **Detección:** alerta automática de movimiento no autorizado.
2. **Verificación:** confirmar la anormalidad mediante datos multisensor.
3. **Notificación:** avisar al equipo de seguridad y responsables de custodia.
4. **Respuesta:** activar protocolos internos (intervención de guardias, bloqueo remoto si aplica).
5. **Notificación a autoridades:** proporcionar datos de ubicación en tiempo real para recuperación.

Estos pasos deben estar documentados y ensayados para que la recuperación del activo sea rápida, organizada y con soporte probatorio suficiente.

6.8 Indicadores de trazabilidad efectiva

Para medir la eficacia del incremento de trazabilidad se pueden usar indicadores cuantitativos y cualitativos:

Indicadores clave

- **Cobertura de sensores:** porcentaje de activos con dispositivos de rastreo habilitados.
- **Exactitud de localización:** precisión promedio de posicionamiento.
- **Tiempo medio de detección de movimiento no autorizado.**
- **Porcentaje de eventos con seguimiento completo hasta resolución.**
- **Integración ERP en tiempo real:** tiempo promedio de actualización en sistemas centrales después de eventos físicos.

Estos indicadores permiten demostrar que la trazabilidad mejora la visibilidad real de los activos y reduce la ventana de explotación por parte de infractores.

6.9 Checklist de implementación

A continuación, un listado operativo para asegurar que el incremento de trazabilidad se implemente correctamente:

Checklist

- ✓ Definición de activos críticos para el rastreo continuo.
- ✓ Selección de tecnologías de identificación y localización (RFID, GPS, BLE, IoT).
- ✓ Diseño de la arquitectura de captura de datos y almacenamiento.
- ✓ Configuración de la plataforma de gestión de activos (software).
- ✓ Integración con ERP y sistemas internos de control.
- ✓ Definición de geocercas y zonas de control autorizadas.
- ✓ Configuración de alertas y canales de notificación.
- ✓ Implementación de protocolos de recuperación ante eventos adversos.
- ✓ Establecimiento de indicadores de trazabilidad efectiva.
- ✓ Auditorías periódicas y calibración de sensores y procesos.

7. COMPONENTE IV — DISUASIÓN COMUNICACIONAL

La *disuasión comunicacional* consiste en el uso deliberado de mensajes, señales y estrategias de comunicación para influir en la percepción y la conducta de individuos potencialmente involucrados en actos delictivos o conductas no deseadas. En el contexto del MNID, su objetivo es aumentar la percepción de riesgo, resaltar consecuencias negativas anticipadas y reducir la percepción de beneficio, actuando directamente sobre los procesos mentales que guían la decisión de delinquir.

Este componente no es solo informativo; es estratégico, psicológico y operativo. Busca cambiar cómo se percibe un entorno, qué asociaciones se hacen con ese entorno y qué decisiones conductuales se toman en base a esa percepción.

7.1 Psicología de la disuasión

La disuasión se basa en teorías psicológicas que muestran que las personas ajustan su conducta en función de percepciones de riesgo y consecuencias, no solo de la realidad objetiva. En criminología, la percepción de ser observado, capturado o juzgado afecta la decisión de cometer un delito.

Mecanismos psicológicos principales

- **Percepción de vigilancia:** Cuando una persona cree que su acción está siendo observada incluso si no lo está, tiende a ajustarse a normas sociales y legales. Por ejemplo, la presencia de cámaras o señalizaciones claras puede reducir comportamientos antisociales simplemente porque los observadores "perciben" mayor probabilidad de detección.
- **Efecto halo de seguridad:** La combinación de múltiples señales de protección (cámaras, guardias, letreros) puede generar un efecto sinérgico que eleva la percepción de riesgo de comisión de delito en el entorno.
- **Asociación social contextual:** Según la teoría de las *ventanas rotas*, los entornos bien mantenidos y percibidos como vigilados reducen la tolerancia social hacia el delito, lo que influye en la percepción de riesgo de los potenciales infractores.

Los mensajes deben ser diseñados no solo para transmitir información, sino para impactar cognitivamente los juicios de probabilidad y consecuencias que hacen las personas antes de actuar.

7.2 Diseño de mensajes estratégicos

Un mensaje estratégico de disuasión debe combinar claridad, relevancia y credibilidad. No es suficiente poner un aviso genérico; hay que diseñar mensajes que:

Componentes de un mensaje eficaz

- **Información de riesgo creíble:** Evidencia numérica o cualitativa de consecuencias reales por comportamientos delictivos (p. ej., "Inmovilización automática y rastreo asegurado").
- **Lenguaje claro y directo:** Evitar ambigüedad, usar frases concisas y comprensibles.
- **Centrado en la audiencia:** Considerar el perfil psicológico, cultural y demográfico del público objetivo.

- **Refuerzo de consecuencias negativas anticipadas:** Resaltar que la acción llevada a cabo tendrá resultados desfavorables (captura, inutilización del bien, registro público).

Ejemplo de mensaje estratégico efectivo

“Este activo está bajo monitoreo continuo con alerta inmediata. Robo o manipulación no autorizada resultará en bloqueo funcional permanente y notificación a autoridades.”

La clave es que el mensaje modifique la percepción del riesgo y el costo de delinquir, no simplemente informar.

7.3 Señalización efectiva en puntos críticos

La señalización es la forma más visible de comunicación preventiva. Cuando se coloca de forma estratégica y coherente, puede servir como recordatorio constante de que el entorno está controlado y que las consecuencias no son triviales.

Principios de señalización efectiva

- **Ubicación estratégica:** Cerca de puntos de acceso, salidas, zonas de alta interacción o áreas de alto riesgo.
- **Diseño visual claro:** Colores contrastantes, símbolos comprensibles, tamaño legible.
- **Mensajes centrados en la percepción de riesgo:** Indicar qué tipo de vigilancia o consecuencia existe (p. ej., “Zona bajo monitoreo 24/7”, “Activación automática de bloqueo en caso de intento de sustracción”).
- **Consistencia con otras señales del entorno:** Evita discrepancias entre lo que el mensaje dice y lo que se observa.

Investigaciones han demostrado que la señalización, al hacer visibles las expectativas de observación y respuesta, puede contribuir a cambios de conducta sin necesidad de aumentos reales en vigilancia.

7.4 Comunicación interna y externa

La disuasión no es solo externa; también debe estar integrada como parte de la cultura organizacional y la relación con stakeholders.

Comunicación interna

- **Capacitación al personal:** Enseñar cómo funcionan las estrategias de prevención y por qué ciertos mensajes están presentes.
- **Participación en mensajes disuasivos:** Integrar mensajes en canales internos (intranets, boletines, capacitaciones) para reforzar la lógica de riesgos y consecuencias.

- **Refuerzo de comportamientos deseados:** Reconocer y comunicar prácticas seguras y preventivas.

Comunicación externa

- **Relación con comunidades y autoridades:** Compartir información sobre estrategias preventivas y resultados puede reforzar la percepción de control y vigilancia.
- **Redes y plataformas públicas:** Uso de canales digitales para difundir mensajes de prevención, alertas y consejos de seguridad.

La comunicación debe ser bidireccional, permitiendo retroalimentación tanto de usuarios internos como de la comunidad, lo cual fortalece su credibilidad.

7.5 Transparencia tecnológica como herramienta preventiva

La transparencia sobre qué tecnologías de seguridad están operando y cómo funcionan puede tener un efecto disuasivo mayor que su simple existencia.

Por ejemplo:

- Indicar que las cámaras están en vivo con monitoreo humano.
- Recordar que los sistemas de bloqueo remoto son reactivos y automáticos.
- Informar sobre sistemas de rastreo y vínculos con autoridades.

Esta transparencia no compromete seguridad si se hace cuidadosamente, pero sí refuerza la percepción real de riesgo y reduce la ilusión de anonimato o impunidad.

La evidencia de campañas de información contextualizada muestra que, cuando las personas perciben que los sistemas no solo existen sino que son efectivos y operativos, cambia su conducta esperada.

7.6 Gestión de reputación disuasiva

Más allá de señales físicas, la reputación de que un entorno, organización o comunidad no tolera el delito influye en la percepción del delito como riesgo.

Estrategias de reputación

- **Publicación de resultados de prevención:** compartir datos de reducción de delitos o incidentes fallidos.
- **Historial de respuesta:** documentar y comunicar cómo se actuó cuando se identificaron amenazas o intentos.
- **Alianzas visibles con autoridades:** reforzar que existe cooperación activa puede elevar la percepción de certeza de consecuencias.

La reputación disuasiva no se construye de la noche a la mañana; se sustenta en coherencia entre mensajes, mecanismos reales y respuesta efectiva.

7.7 Medición de percepción de riesgo

Para evaluar si las estrategias de disuasión comunicacional están funcionando, se debe medir cómo cambia la percepción de riesgo entre distintos grupos objetivo (potenciales infractores, empleados, clientes).

Métodos comunes

- **Encuestas directas:** preguntar sobre percepción de riesgo antes y después de campañas o señalizaciones.
- **Grupos focales con perfiles relevantes.**
- **Análisis de comportamiento:** cambios en patrones de incidentes luego de implementar mensajes.

La percepción de riesgo no siempre coincide con indicadores objetivos de riesgo; sin embargo, es clave para la toma de decisiones del individuo. Un aumento en percepción de riesgo suele traducirse en reducción de conducta delictiva.

7.8 Indicadores de impacto conductual

Los indicadores permiten saber si la disuasión comunicacional está alterando conductas relevantes.

Indicadores principales

- **Cambio en el número de incidentes** en áreas con señalización activa.
- **Variación en la percepción de riesgo** medida en períodos específicos.
- **Tasa de intentos versus éxitos de conducta delictiva** luego de campañas informativas.
- **Visibilidad y reconocimiento de mensajes** (evaluado con encuestas).
- **Engagement con mensajes externos** en redes o plataformas públicas.

Estos indicadores deben ser monitoreados en forma continua y comparados con períodos previos para analizar tendencias.

7.9 Checklist de implementación

Para asegurar que la disuasión comunicacional se implemente de forma eficaz, sigue este checklist operativo:

Checklist

- ✓ Definir públicos objetivos de los mensajes (potenciales infractores, empleados, comunidad).
- ✓ Diseñar mensajes estratégicos basados en percepción de riesgo y consecuencias.
- ✓ Establecer señalización en puntos críticos con diseño visual y textual coherente.

- ✓ Integrar mensajes en comunicación interna (boletines, capacitaciones, carteles).
- ✓ Desarrollar estrategia de comunicación externa (redes, web, alianzas con autoridades).
- ✓ Transparentar tecnologías de seguridad operativas sin comprometer su eficacia.
- ✓ Promover gestión de reputación disuasiva con publicación de resultados.
- ✓ Medir percepción de riesgo antes y después de intervenciones.
- ✓ Monitorear indicadores de impacto conductual regularmente.
- ✓ Ajustar mensajes según resultados y retroalimentación.

COMPONENTE V – SUSTITUCIÓN DEL INCENTIVO

El objetivo del componente de Sustitución del Incentivo es intervenir en las condiciones estructurales y socioeconómicas que pueden motivar o facilitar la comisión de delitos patrimoniales u otras conductas delictivas. Mientras los otros componentes del MNID reducen la oportunidad, el valor funcional y comercial, y elevan riesgos, este componente busca cambiar las condiciones del entorno para que delinquir sea menos atractivo, no solo desde el costo-beneficio inmediato, sino desde la situación de vida y opciones disponibles para los actores. Esto no se limita a la sanción o a la herramienta tecnológica: es una intervención de raíz, orientada a reducir las presiones que empujan a la conducta delictiva.

Este enfoque se basa en la idea de que las condiciones sociales —como pobreza, desempleo, exclusión o falta de oportunidades— pueden crear una “presión estructural” que incrementa la probabilidad de conductas delictivas. La sustitución del incentivo, por lo tanto, busca ofrecer alternativas legítimas y deseables que reduzcan la motivación para delinquir y fortalezcan capacidades y recursos sociales.

8.1 Identificación de motivaciones estructurales

Antes de diseñar estrategias, es esencial identificar las motivaciones estructurales profundas que incrementan la probabilidad de involucrarse en comportamientos delictivos.

Entre estas motivaciones se encuentran:

Factores económicos

- **Desempleo o subempleo**: falta de ingresos legítimos puede llevar a buscar ingresos ilegales.
- **Pobreza**: necesidad básica insatisfecha aumenta la presión sobre familiares y comunidades.

- **Desigualdad económica**: brechas amplias entre clases sociodemográficas pueden generar resentimiento y oportunidades para el delito.

Factores sociales

- **Exclusión social**: personas marginadas con pocas redes de apoyo tienen menos barreras hacia conductas ilícitas.
- **Falta de capital social y cohesión comunitaria**: entornos donde no existen conexiones fuertes entre vecinos y grupos sociales facilitan el surgimiento de actividades antisociales.

Factores culturales

- **Normas y percepciones sobre la legalidad**: entornos con baja legitimidad del sistema legal pueden percibir el delito como un medio “aceptable” para obtener beneficios.

Este análisis debe realizarse con datos locales y, preferiblemente, con un enfoque diferencial (edad, género, contexto comunitario) para comprender qué empuja a diversos grupos hacia la conducta delictiva.

8.2 Análisis socioeconómico del entorno

Una vez identificadas motivaciones estructurales, se debe realizar un análisis socioeconómico del entorno para comprender mejor el contexto en el que estas motivaciones operan. Este análisis evalúa variables como:

Empleo y oportunidades económicas

- Tasa de desempleo y subempleo.
- Distribución de empleos formales versus informales.
- Accesibilidad a programas de capacitación laboral.

Condiciones de vida

- Condiciones de vivienda y servicios básicos.
- Acceso a educación y servicios de salud.
- Infraestructura comunitaria y espacios públicos.

Capital social y cohesión comunitaria

- Existencia de organizaciones vecinales o comunitarias.
- Redes de apoyo y vínculos interpersonales.
- Participación en actividades colectivas.

Este tipo de análisis ayuda a identificar qué factores estructurales son más determinantes en una comunidad determinada y a priorizar las estrategias de sustitución de incentivos que deben implementarse.

8.3 Estrategias de reducción de presión económica

Una forma directa de sustituir el incentivo delictivo es implementar estrategias que reduzcan la presión económica y abran alternativas legítimas de ingresos, tales como:

Empleo subsidiado y formación laboral

Programas que combinan empleo con capacitación profesional pueden reducir la probabilidad de participación en conductas delictivas. Un ejemplo es el enfoque de empleo subsidiado más terapia conductual para población en riesgo, que ha mostrado resultados prometedores en ciudades de Estados Unidos al aumentar oportunidades económicas para personas con riesgo de involucrarse en violencia.

Educación y capacitación técnica

La incorporación de jóvenes y adultos desempleados a programas de educación técnica y certificación puede ofrecerles caminos legítimos para el desarrollo profesional, reduciendo la necesidad de buscar ingresos ilegales.

Red de apoyo económico y servicios sociales

El fortalecimiento de la red de asistencia social (apoyo alimentario, salud, subsidios) puede aliviar la presión económica inmediata que impulsaría a algunas personas a delinquir.

Estas estrategias buscan aumentar el costo de oportunidad de delinquir, haciendo que la participación en actividades legítimas sea más atractiva y sostenible.

8.4 Programas de recompra o regularización

Los programas de recompra (buyback) y regularización son intervenciones que buscan reducir la circulación de bienes que puedan ser utilizados en actividades delictivas o ofrecer incentivos para que personas dejen de involucrarse en redes delictivas a cambio de beneficios legítimos.

Un ejemplo clásico es el programa de recompra de armas, donde personas entregan voluntariamente armas a cambio de incentivos económicos o bienes básicos. Este enfoque busca reducir la disponibilidad de instrumentos que facilitan crímenes violentos y, aunque su impacto puede variar, ha sido ampliamente utilizado como herramienta de reducción de armas en cirucitos comunitarios.

En el contexto del MNID, estos programas pueden ampliarse a bienes vinculados a delitos patrimoniales u otros instrumentos que incrementan el riesgo de reincidencia, reduciendo así el incentivo de su posesión a largo plazo.

8.5 Integración comunitaria y responsabilidad social

Las estrategias de sustitución del incentivo deben incluir acciones que fortalezcan la integración comunitaria y la responsabilidad social a través de:

Programas comunitarios y participación vecinal

La participación activa de vecinos y organizaciones locales en la solución de problemas de seguridad fortalece el capital social y fomenta condiciones de convivencia que reducen tendencias delictivas.

Alianzas público-privadas y ONGs

Colaboraciones entre gobiernos, sector privado y organizaciones civiles pueden financiar proyectos de desarrollo, empleo, capacitación y espacios comunitarios que ofrezcan alternativas legítimas a la criminalidad.

Actividades culturales y recreativas

Iniciativas deportivas, artísticas o recreativas dirigidas a jóvenes en riesgo pueden ofrecer oportunidades de inclusión positiva, reduciendo el tiempo y la motivación para delinquir.

Este tipo de integración aumenta la cohesión social y crea entornos menos propensos a la ocurrencia de delitos.

8.6 Modelos de acceso formal alternativo

Además de reducir incentivos negativos, la sustitución implica crear o fortalecer canales formales de acceso legítimo a recursos y oportunidades:

Bolsas de empleo y ferias laborales locales

Promover ferias donde empresas y organizaciones ofrecen puestos de trabajo adaptados a población en riesgo.

Programas de emprendimiento

Apoyo a microempresas y iniciativas productivas locales, con acceso a crédito y capacitación técnica.

Pasantías y transferencias educativas

Vincular a jóvenes a programas educativos y de inserción laboral temprana para reducir la probabilidad de involucrarse en delitos.

Estas estrategias ayudan a construir caminos viables de desarrollo personal y económico, reduciendo la percepción de que el delito es la única alternativa disponible.

8.7 Prevención de desplazamiento del delito

Un desafío central de cualquier intervención para reducir el delito es el fenómeno conocido como desplazamiento del delito, donde la actividad delictiva se traslada a otras zonas, horarios o modalidades, en lugar de ser eliminada. Por ejemplo, al incrementar la vigilancia en una colonia, los delincuentes pueden migrar hacia áreas menos vigiladas o

cambiar de tipo de delito, pasando de robos a fraudes digitales. Por esta razón, las estrategias de sustitución deben estar diseñadas para anticipar y contrarrestar estas posibles adaptaciones.

Diseñarse de forma integral

Es fundamental que las estrategias combinen apoyos económicos, oportunidades de educación, acceso a empleo formal y fortalecimiento de la cohesión social. De esta manera, no solo se eliminan incentivos negativos, sino que se ofrecen alternativas legítimas y sostenibles para el desarrollo personal y colectivo. Además, la colaboración interinstitucional entre gobierno, sector privado y organizaciones civiles puede maximizar el impacto y cobertura de los programas, evitando vacíos que permitan el desplazamiento del delito.

Monitoreo constante

Es imprescindible implementar sistemas de evaluación y monitoreo permanente, utilizando indicadores tanto cuantitativos como cualitativos para analizar si las intervenciones están logrando disminuir los delitos o si, por el contrario, están generando desplazamientos hacia otros contextos o formas. Herramientas como mapas de calor delictivo, encuestas comunitarias y análisis de tendencias pueden ayudar a detectar y corregir estos cambios oportunamente.

El enfoque de prevención social reconoce que las causas del delito son múltiples y complejas, incluyendo factores económicos, educativos y sociales. Por ello, es necesario abordarlas desde diferentes frentes, evitando soluciones aisladas que solo trasladen el problema. La participación activa de la comunidad y la adaptación constante de las estrategias, basándose en evidencia y retroalimentación, son claves para evitar resultados contraproducentes y lograr una reducción genuina de la actividad delictiva.

8.8 Indicadores de reducción estructural

Los indicadores usados para evaluar el impacto de estas estrategias deben reflejar cambios estructurales y sociales:

Indicadores económicos

- Tasa de empleo formal en la población objetivo.
- Variación del ingreso promedio en zonas de intervención.
- Número de personas incorporadas a programas de capacitación o empleo.

Indicadores sociales

- Nivel de participación comunitaria en programas sociales y preventivos.
- Medición de cohesión social (confianza vecinal, redes locales).
- Reducción de la percepción de desempleo forzado como motivación de delito.

Indicadores de criminalidad

- Reducción de tasas de reincidencia o intentos de delitos patrimoniales en poblaciones atendidas.
- Disminución de la proporción de delitos asociados a carencia económica.

Estos indicadores permiten medir cómo las condiciones estructurales han cambiado, no solo cómo ha cambiado el número de delitos.

8.9 Checklist de implementación

Aquí tienes una lista operativa de verificación para asegurar que el componente de sustitución del incentivo se implementa correctamente:

Checklist

- ✓ Realizar diagnóstico de motivaciones estructurales en comunidad objetivo.
- ✓ Conducir análisis socioeconómico del entorno con datos cuantitativos y cualitativos.
- ✓ Diseñar estrategias de reducción de presión económica adaptadas a los hallazgos.
- ✓ Evaluar viabilidad de programas de recompra o regularización según contexto.
- ✓ Establecer alianzas con actores comunitarios, sector privado y gobierno.
- ✓ Implementar modelos de acceso formal alternativo (empleo, educación, emprendimiento).
- ✓ Diseñar mecanismos de prevención de desplazamiento del delito.
- ✓ Establecer indicadores base para medir reducción estructural.
- ✓ Ejecutar seguimiento y evaluación periódica.
- ✓ Ajustar estrategias con base en evidencia de impacto y retroalimentación.

9. INTEGRACIÓN SISTÉMICA DEL MNID

La integración sistémica del MNID consiste en articular y sincronizar los cinco componentes del modelo —Desvalorización Funcional, Desvalorización Comercial, Incremento de Trazabilidad, Disuasión Comunicacional y Sustitución del Incentivo— de forma cohesiva, coherente y compatible con la gestión organizacional y los marcos de riesgo y compliance existentes. Esto implica establecer fases de implementación, estructuras de gobernanza, roles claros, coordinación interna y externa, mecanismos de monitoreo y evaluación y vinculación con normas globales como ISO 31000 para maximizar eficacia, sostenibilidad y alineación estratégica con los objetivos institucionales.

9.1 Modelo de implementación por fases

Un modelo de implementación por fases asegura que la adopción del MNID sea estructurada, ordenada y medible. Una implementación típica puede contener las siguientes etapas:

1. **Preparación y alineación estratégica**
    - Sensibilización de líderes y stakeholders.
    - Definición de alcance y objetivos del MNID.
    - Evaluación de contexto organizacional y riesgos.
2. **Diagnóstico y diseño**
    - Identificación de activos, vulnerabilidades y motivaciones delictivas.
    - Diseño de políticas, protocolos y marcos de medición.
    - Planificación de recursos y cronogramas.
3. **Pilotaje y despliegue inicial**
    - Prueba de componentes en áreas críticas antes de una implementación amplia.
    - Ajuste de tecnologías, comunicaciones y métricas.
4. **Implementación integral**
    - Ejecución de todos los mecanismos del MNID.
    - Formación, capacitación, señalización, integración de sistemas y registro de datos.
5. **Monitoreo, evaluación y mejora continua**
    - Uso de indicadores y sistemas de auditoría.
    - Retroalimentación y ajustes periódicos de estrategia.

Cada fase debe tener metas y criterios de salida claros, con documentos de seguimiento, reuniones de evaluación y decisiones formales para avanzar a la siguiente etapa.

9.2 Sincronización de los cinco componentes

La sincronización de los cinco componentes del MNID es fundamental para garantizar una operación sistémica eficiente, donde cada elemento refuerza a los demás y se evitan duplicidades, lagunas o contradicciones. Un sistema integrado permite que los flujos de información, recursos y decisiones sean ágiles y coherentes, facilitando la prevención y gestión de riesgos de manera proactiva.

a) Compatibilidad de acciones: Asegurar que las estrategias y actividades de cada componente no solo sean congruentes entre sí, sino que se potencien mutuamente. Esto implica una revisión periódica de los objetivos, metodologías y resultados esperados,

promoviendo la alineación mediante sesiones de trabajo colaborativo y la creación de protocolos compartidos.

b) Coordinación logística: Es esencial establecer mecanismos para la planeación conjunta, asignación de recursos y calendarización de actividades. La logística debe contemplar la optimización de tiempos, el uso eficiente de infraestructura y la disponibilidad de personal clave, así como la gestión de imprevistos a través de canales de comunicación claros y jerarquizados.

c) Modelo de datos unificado: El desarrollo de un modelo de datos unificado es crucial para alimentar una base común de conocimiento que permita análisis integrados de riesgo y decisiones informadas. Esto requiere la homologación de formatos de captura, la interoperabilidad de sistemas y la adopción de estándares para el resguardo y uso de la información, garantizando confidencialidad y acceso oportuno para quienes toman decisiones.

d) Enfoque adaptativo: Adoptar un enfoque adaptativo implica que el sistema esté preparado para ajustar procesos, recursos y estrategias conforme se identifican nuevas necesidades, riesgos emergentes o cambios en el contexto. La flexibilidad institucional y la promoción de una mentalidad de mejora continua son clave para mantener la vigencia y efectividad del modelo.

Esta sincronización se asemeja a los marcos de gestión de riesgos empresariales y de calidad, como el estándar ISO 31000, donde la integración, el liderazgo y la mejora continua son pilares para la eficacia organizacional. Un sistema bien sincronizado reduce la fragmentación, mejora la toma de decisiones y facilita el cumplimiento de objetivos estratégicos.

9.3 Gestión del cambio organizacional

La introducción del MNID representa una transformación profunda que trasciende los aspectos tecnológicos u operativos, ya que impacta la cultura y las dinámicas institucionales. La gestión del cambio es un proceso sistemático que debe contemplar la preparación de la organización, la gestión de resistencias y la consolidación de nuevos hábitos y valores.

- **Liderazgo visible:** El involucramiento activo de la alta dirección y mandos intermedios es indispensable para legitimar el proceso y motivar la participación de todo el personal. Se recomienda establecer un comité de cambio que dé seguimiento y resuelva obstáculos.
- **Comunicación efectiva:** Se deben implementar campañas y espacios de diálogo abiertos, utilizando diversos canales (presenciales y digitales) para mantener informada a la organización sobre los objetivos, avances y beneficios del MNID, así como para atender dudas y sugerencias.
- **Capacitación y desarrollo:** Es vital diseñar programas de formación continua, talleres prácticos y materiales didácticos que permitan a todos los niveles

comprender sus nuevos roles y responsabilidades, y cómo estos aportan al éxito del modelo.

- **Cultura de prevención:** Fomentar una cultura organizacional donde la seguridad, la prevención y el reporte de incidentes sean valores centrales. Esto implica reconocer y recompensar comportamientos preventivos, así como establecer mecanismos de retroalimentación y mejora.

La gestión del cambio debe ser estructurada, con responsables designados, cronogramas claros, canales de comunicación efectivos y métricas para evaluar la adopción cultural. Es recomendable realizar diagnósticos previos, encuestas de clima organizacional y ajustes periódicos a la estrategia de cambio, siguiendo buenas prácticas internacionales como el modelo ADKAR o el enfoque de Kotter.

9.4 Gobernanza del modelo

La gobernanza define la estructura de dirección, supervisión y toma de decisiones del MNID. Incluye:

- Órganos colegiados o comités de seguridad y prevención.
- Políticas claras de aprobación, evaluación y sanción.
- Enlaces entre unidades organizacionales para evitar silos funcionales.

Una buena gobernanza asegura que el modelo sea sostenible, que las decisiones se tomen con información robusta y que exista rendición de cuentas. Esto implica también mecanismos deliberativos, evaluación de intereses y ajuste continuo de estrategias con evidencia (como indica la gestión pública de prevención de violencia y delincuencia).

9.5 Roles y responsabilidades

Definir roles, autoridades y responsabilidades es indispensable para que el MNID funcione:

- **Alta dirección:** liderazgo estratégico, asignación de recursos y legitimación institucional.
- **Comité de gobernanza de riesgos:** supervisión global, revisión de indicadores y decisiones de alto nivel.
- **Gestores de riesgos y de componentes específicos:** responsables operativos de cada componente del modelo.
- **Auditoría interna:** evaluación independiente de cumplimiento y eficacia.
- **Usuarios y empleados base:** cumplimiento, reporte de incidentes y retroalimentación.

Según los principios de ISO 31000, los roles deben estar claramente documentados, actualizados y alineados con la gobernanza corporativa para asegurar responsabilidad y transparencia en la gestión de riesgos.

9.6 Integración con ISO 31000 y gestión de riesgos

Integrar el MNID con un marco de gestión de riesgos formal como ISO 31000 aporta robustez metodológica. ISO 31000:

- Proporciona principios y directrices para identificar, evaluar y tratar riesgos.
- Enfatiza la adaptación del marco de riesgo a la estructura y objetivos organizacionales.
- Promueve la integración del riesgo en la gobernanza y cultura empresarial, incluyendo liderazgo y políticas.

Al alinear el MNID con ISO 31000, se obtiene:

- Consistencia en la evaluación y tratamiento de riesgos.
- Estándares comunes para medir impacto e implementar controles.
- Integración con procesos de planificación, evaluación y monitoreo de riesgos organizacionales.

En otras palabras, el modelo se convierte en parte de la gestión integral de riesgos de la organización, no en un conjunto aislado de acciones.

9.7 Integración con compliance y auditoría

La gestión del MNID debe articularse con los mecanismos de cumplimiento normativo (compliance) y auditoría interna/external para asegurar:

- Cumplimiento de leyes, normas y estándares aplicables al sector.
- Evaluaciones periódicas objetivas del funcionamiento del modelo.
- Detección temprana de deficiencias o brechas operativas.
- Preparación para auditorías externas y exigencias regulatorias.

Esto implica que las políticas, procedimientos y registros del MNID se documenten, mantengan y auditen como parte del sistema de compliance organizacional.

9.8 Plan maestro de despliegue

Un plan maestro de despliegue es un documento estructurado que:

1. **Define objetivos y metas** del MNID a corto, mediano y largo plazo.
2. **Especifica fases de implementación**, recursos, tiempos y responsables.
3. **Establece métricas e indicadores** para evaluar progreso.

4. **Detalla los mecanismos de coordinación entre áreas.**
5. **Incluye la gestión del cambio** y actividades de capacitación.
6. **Contempla revisiones periódicas y procesos de mejora.**

Este plan se concibe como la hoja de ruta para que el MNID se consolide, se ajuste según evidencia y se mantenga vigente en el tiempo. Se construye con aportes de todas las áreas involucradas, desde operaciones hasta auditoría y compliance, asegurando una visión integral y sostenible.

Resumen
La integración sistémica del MNID transforma un conjunto de buenas prácticas aisladas en un sistema alineado con la estrategia organizacional, gobernanza y gestión de riesgos. Al adoptar un enfoque por fases, establecer gobernanza sólida, definir roles claros, integrar con marcos reconocidos como ISO 31000 y conectar con compliance y auditoría, la organización no solo reduce incentivos delictivos, sino que se fortalece integralmente frente a riesgos actuales y emergentes.

10. MATRICES Y HERRAMIENTAS OPERATIVAS

Las matrices y herramientas operativas del MNID son instrumentos prácticos y cuantificables que traducen análisis complejos en formatos ejecutables. Estas herramientas permiten evaluar, priorizar, monitorear y auditar riesgos, incentivos y la efectividad de las acciones del modelo de forma sistemática y repetible.

10.1 Matriz de Incentivo Delictivo (MID)

¿Qué es?

La Matriz de Incentivo Delictivo (MID) es una tabla que cruza las variables clave para determinar cuánto «atractivo» tiene un activo para un potencial infractor, considerando no solo su valor económico sino la facilidad de monetización, vulnerabilidades y percepción de riesgo.

Componentes típicos

Activo	Valor real	Valor de mercado informal	Vulnerabilidades (1–5)	Riesgo percibido (1–5)	Monetización fácil (1–5)	Índice de atractivo

Valor real es el impacto para la organización;
Valor de mercado informal es cuánto podría obtener un delincuente por el bien robado;
Vulnerabilidades mide la facilidad de acceso o explotación;
Riesgo percibido estima la probabilidad de detección según controles existentes;
Monetización fácil mide qué tan sencillo es convertir el botín en dinero o bienes.

Interpretación

La matriz puede producir un índice de atractivo ponderado que ayuda a priorizar activos que requieren intervenciones del MNID. Su estructura permite decisiones estratégicas y operacionalización de prioridades.

10.2 Matriz de Cadena de Monetización

¿Qué es?

Es una herramienta que representa cada eslabón del proceso mediante el cual un bien robado se transforma en dinero o utilidad para el infractor o el mercado informal.

Estructura básica — ejemplo

Eslabón	Descripción	Actores	Valor añadido	Riesgo de intervención	Indicadores
Sustracción	Robo físico del bien	Infractor	100%	% detectado	Incidentes / total
Traslado	Movimiento fuera del entorno	Infractor / transporte	~90%	GPS / trazabilidad	Eventos rastreados
Intermediación	Venta a «fence» / comprador informal	Intermediario	~70%	Verificación pública	Casos frenados
Reventa	Venta al usuario final	Comprador	~50%	Registro público	Transacciones bloqueadas

Esta matriz permite identificar puntos críticos donde neutralizar el incentivo (p. ej., dificultar monetización) y qué herramientas o acciones del MNID (p. ej., trazabilidad, registro público) aplican en cada fase.

10.3 Matriz de Neutralización Progresiva

¿Qué es?

Una matriz que muestra cómo las acciones de cada componente del MNID (Desvalorización funcional, comercial, trazabilidad, disuasión, sustitución) van reduciendo progresivamente el incentivo delictivo del activo.

Ejemplo simplificado

Componente MNID	Acción	Resultado esperado	Nivel de incentivo antes	Nivel de incentivo después
Funcional	Bloqueo remoto	No se puede usar el bien	Alto	Medio

Comercial	Marcaje permanente	Mercado de reventa limitado	Medio	Bajo
Trazabilidad	GPS IoT	Se puede ubicar al activo robado	Bajo	Muy bajo
Disuasión	Señalización + campañas	Percepción de riesgo alto	Muy bajo	Nulo
Sustitución	Programas socioeconómicos	Reducción motivación estructural	Nulo	Negligible

Esta matriz muestra cómo se reduce el atractivo del activo en cada etapa mediante la agregación de controles, hasta llegar a un nivel donde su robo ya no resulta rentable ni deseable para los infractores.

10.4 Evaluación costo–beneficio del MNID

¿Qué es?

Una herramienta que compara costos de implementación de controles y acciones del MNID con los beneficios estimados (p. ej., valor de pérdidas evitadas, reducción de incidentes, mejora reputacional, ahorro en seguros).

Metodologías usuales

Indicadores financieros usados:

- *Retorno de la inversión en seguridad (ROSI)* = (Beneficios − Costos de Implementación) / Costos × 100
- *Valor presente neto (VPN)* de beneficios futuros descontados
- *Período de recuperación* del gasto inicial

Ejemplo de aplicación

Si un control reduce un tipo de robo que genera pérdidas anuales estimadas de $100,000 y cuesta $30,000 instalarlo y operar por año, el cálculo de ROSI ayuda a justificar la inversión.

10.5 Modelo de priorización de activos

¿Qué es?

Un modelo que ayuda a decidir **en qué activos intervenir primero** basándose en múltiples criterios, como criticidad, valor en mercado informal, vulnerabilidad, impacto operativo y facilidad de monetización.

Ejemplo de matriz ponderada

Activo	Criticidad estratégica (1–5)	Vulnerabilidad (1–5)	Valor de mercado informal (1–5)	Prioridad total
Activo A	5	4	5	14
Activo B	3	2	3	8

Cada criterio se pondera (p. ej., criticidad ×2, vulnerabilidad ×1.5, valor ≈1), permitiendo una priorización objetiva y alineada con los objetivos de mitigación. Esta práctica es común en gestión de riesgos operativos y seguridad corporativa.

10.6 Dashboard de indicadores

¿Qué es?

Un tablero de control visual que integra indicadores clave de desempeño y de riesgo para monitorear la implementación y resultados del MNID en tiempo real.

Indicadores típicos

- Incidentes detectados vs. mitigados
- Porcentaje de activos con trazabilidad activa
- Valor de reventa estimado antes/después de controles
- Tiempos de detección de eventos no autorizados
- Percepción de riesgo medido en encuestas internas/external

El dashboard puede construirse con herramientas como Power BI, Tableau o sistemas integrados de gestión de seguridad, y permite tomar decisiones ágiles y basadas en datos confiables.

10.7 Formatos de auditoría MNID

¿Qué son?

Son plantillas y formatos documentales para registrar auditorías internas o externas sobre la implementación y cumplimiento de cada componente del modelo.

Elementos típicos del formato de auditoría

1. **Identificación del auditor**
2. **Alcance de la auditoría**
3. **Componentes revisados**
    - Desvalorización funcional
    - Comercial

- Trazabilidad
- Disuasión
- Sustitución

4. **Hallazgos**
    - Cumplimiento (Sí/No/Parcial)
    - Evidencias documentales
    - Evidencias físicas
5. **Brechas encontradas**
6. **Recomendaciones**
7. **Plan de acción y responsable**
8. **Fechas de seguimiento**

Estos formatos suelen integrarse en el sistema de gestión de riesgos y compliance de la organización para asegurar que las acciones del MNID sean auditables, verificables y mejorables con el tiempo.

Resumen

Las matrices y herramientas operativas del MNID son la columna vertebral cuantitativa del modelo. Permiten:

- Tomar decisiones objetivas basadas en datos concretos.
- Priorizar acciones y recursos en función del riesgo e incentivo.
- Monitorear y medir resultados con claridad.
- Auditar y mejorar continuamente los procesos de prevención.

Estas herramientas se integran con prácticas reconocidas de gestión de riesgos y seguridad corporativa, adaptadas a la lógica específica de neutralizar incentivos delictivos y proteger el patrimonio de forma estratégica y sostenible.

11. INDICADORES Y MEDICIÓN DE IMPACTO

La medición de impacto es un pilar fundamental para validar la eficacia del Modelo de Neutralización de Incentivo Delictivo (MNID) en contextos corporativos y de seguridad patrimonial. Una gestión de riesgos moderna exige demostrar, con datos objetivos y trazables, que las intervenciones implementadas realmente disminuyen la exposición a delitos, reducen el valor esperado para el infractor y protegen los activos críticos. Por ello, el uso de indicadores clave de desempeño (KPIs) estratégicos y operativos, alineados con buenas prácticas internacionales como las propuestas por ISO 31000 (gestión de riesgos), ISO 22301 (resiliencia organizacional) y metodologías de evaluación de

programas de prevención del delito (Crime Prevention Through Environmental Design, CPTED; CompStat), es esencial para la toma de decisiones informadas, la mejora continua y la rendición de cuentas ante la alta dirección.

Para una gestión integral, los indicadores se segmentan en dos grandes categorías complementarias:

1. **KPIs estratégicos** : Evalúan el impacto macro y la contribución del MNID a los objetivos institucionales de seguridad, continuidad de negocio y reputación.
2. **KPIs operativos** : Miden la eficiencia, cobertura y eficacia de los procesos, controles y acciones tácticas implementadas en el día a día.

La correcta selección, monitoreo y análisis de estos indicadores permite a los directivos identificar tendencias, anticipar riesgos emergentes y asignar recursos de forma óptima.

11.1 KPIs estratégicos

Los indicadores estratégicos proporcionan una visión global del desempeño del MNID y su alineación con la visión organizacional. Se enfocan en resultados de alto impacto y permiten comparar la evolución frente a metas anuales, benchmarks sectoriales y tendencias históricas. Entre los más relevantes para la seguridad patrimonial se encuentran:

- **Tasa de incidencia delictiva total** (delitos por cada 100,000 habitantes o eventos por unidad operativa). Su reducción refleja la efectividad sistémica de la estrategia de prevención.
- **Reducción porcentual de delitos patrimoniales clave** (año contra año o periodo equivalente). Permite medir la mejora específica en los activos más críticos.
- **Porcentaje de activos con controles de neutralización implementados** respecto del total de activos críticos, midiendo la cobertura y madurez de la estrategia.
- **Valor estimado mitigado de pérdida patrimonial** , calculado a partir de incidentes frustrados y recuperaciones, útil para justificar inversiones en seguridad.
- **Percepción de seguridad entre usuarios y empleados** , evaluada mediante encuestas estructuradas, pues la confianza es clave para la cultura de prevención.

Estos KPIs se interpretan mediante análisis comparativos, revisión de tendencias y evaluación de cumplimiento de objetivos estratégicos. Su utilidad radica en orientar la estrategia general, priorizar intervenciones y reportar resultados a la alta dirección y stakeholders.

11.2 KPIs operativos

Los KPIs operativos permiten monitorear la eficiencia de los controles, detectar áreas de mejora inmediata y mantener la disciplina operativa. Son clave para la gestión táctica y el ciclo de mejora continua. Entre los indicadores operativos más efectivos destacan:

- **Número de incidentes detectados por mecanismos de trazabilidad** (sensores, bitácoras, sistemas de alarmas).
- **Tiempo medio de detección de eventos no autorizados (MTTD)** , indicador de agilidad de monitoreo.
- **Tiempo medio de reacción o respuesta (MTTR)** tras detección, crítico para mitigar pérdidas y daños.
- **Proporción de bienes recuperados tras detección en comparación con intentos totales** , útil para evaluar la efectividad de las respuestas y procesos de recuperación.
- **Porcentaje de fallos de control o bypass detectados durante auditorías internas** , para medir la robustez y confiabilidad de los controles.
- **Porcentaje de personal o usuarios que completó la capacitación de prevención** , indicador de madurez cultural y cobertura de sensibilización.

La interpretación de estos KPIs operativos permite identificar cuellos de botella, brechas en la implementación y oportunidades de mejora inmediata, contribuyendo a la resiliencia organizacional.

11.3 Metodologías de medición y mejores prácticas

Para asegurar comparabilidad, objetividad y utilidad gerencial, las mejores prácticas internacionales recomiendan:

- **Definir líneas base y metas claras:** Recopilar datos previos a la implementación del MNID y establecer metas SMART (específicas, medibles, alcanzables, relevantes y temporales).
- **Comparar periodos equivalentes:** Para evitar sesgos estacionales o de contexto, se recomienda comparar periodos homogéneos (ejemplo: año contra año, trimestre contra trimestre).
- **Utilizar fórmulas estandarizadas:** Por ejemplo, tasa de intento = (número de intentos / universo de exposición) × 100; tasa de éxito delictivo = (eventos exitosos / intentos totales) × 100.
- **Análisis de tendencias y segmentaciones:** Uso de gráficos de control, curvas de tendencia y análisis por segmento de activo, zona o periodo.
- **Interpretar contexto y factores externos:** Incluir variables como cambios regulatorios, hechos sociales relevantes o innovaciones tecnológicas.

Estas metodologías fortalecen la credibilidad de los resultados y facilitan la auditoría y mejora continua del MNID, alineando el proceso con estándares como COSO ERM y recomendaciones de la OCDE en integridad corporativa.

11.4 Ejemplos integrados de KPIs para seguridad patrimonial

- **Reducción de tasa de intento:** Compara la frecuencia de intentos de delito antes y después del MNID. Fundamental para medir el efecto disuasivo del modelo.
- **Reducción de éxito delictivo:** Identifica la proporción de intentos exitosos versus frustrados. Un descenso relevante justifica la inversión en controles.
- **Tiempo de monetización ilegal:** Mide el promedio de días entre la sustracción y la venta/utilización en canales informales. Un aumento en este tiempo implica menor incentivo económico para el infractor.
- **Variación en valor de mercado negro:** Analiza la disminución del precio promedio de activos robados en mercados secundarios tras implementar controles, apoyando la estrategia de desvalorización comercial.

La combinación de estos indicadores permite una evaluación integral y comparativa de la eficacia del MNID.

11.5 Reportes ejecutivos y utilidad para la toma de decisiones

Los reportes ejecutivos deben estructurarse de forma clara, visual y orientada a la acción. Una estructura recomendada incluye: resumen de resultados clave, gráficas comparativas pre y post implementación, análisis de brechas (metas no alcanzadas y causas), recomendaciones estratégicas y contexto de gestión de riesgos. Además, se recomienda incorporar dashboards interactivos y semáforos de alerta para facilitar la toma de decisiones rápida y el seguimiento por parte de comités de riesgos y gobernanza.

11.6 Integración de indicadores en la gestión estratégica

La integración sistemática de KPIs y metodologías de medición en el MNID fortalece la gestión estratégica de riesgos y la protección patrimonial. Permite tomar decisiones fundamentadas en evidencia, ajustar tácticas y estrategias de seguridad, demostrar la eficacia de las intervenciones y alinear la prevención del delito con los objetivos organizacionales de valor, resiliencia y cumplimiento normativo. La actualización y revisión periódica de los indicadores garantiza su vigencia y pertinencia ante la evolución del entorno de amenazas.

En conclusión, la medición de impacto mediante KPIs estratégicos y operativos, sustentada en metodologías robustas y reportes ejecutivos claros, es indispensable para la efectividad, mejora continua y legitimidad del Modelo de Neutralización de Incentivo Delictivo en entornos corporativos y de seguridad patrimonial.

12. Gestión de riesgos y adaptación criminal

La gestión de riesgos es un proceso sistemático y estructurado que permite a las organizaciones identificar, analizar, evaluar y responder a factores que pueden afectar el logro de sus objetivos estratégicos, operativos o misionales. En el contexto de la seguridad corporativa y la prevención del delito, la gestión de riesgos no solo implica anticipar vulnerabilidades en los activos o procesos protegidos, sino también prever y comprender cómo los infractores pueden modificar su comportamiento para sortear los controles implementados. Este enfoque, fundamentado en marcos internacionales como ISO 31000 y la gestión integral de riesgos (ERM), es esencial para diseñar estrategias de protección patrimonial efectivas y sostenibles.

La adaptación criminal es un concepto central en la criminología contemporánea que reconoce la capacidad de individuos y redes delictivas para aprender, modificar conductas y adoptar nuevas tácticas frente a la evolución de las medidas preventivas. Los infractores no son actores pasivos; analizan el entorno, detectan debilidades en los sistemas de control y desarrollan respuestas innovadoras para mantener sus beneficios ilícitos. Un ejemplo claro es la migración de delitos tradicionales hacia modalidades digitales tras el refuerzo de controles físicos. Ignorar la adaptabilidad criminal puede llevar a una falsa sensación de seguridad y al fracaso de las estrategias de prevención. Por ello, la gestión de riesgos debe incorporar análisis prospectivos y monitoreo constante de las tendencias delictivas, así como fomentar una cultura organizacional de resiliencia y anticipación.

12.1 Posible desplazamiento del delito

El *desplazamiento del delito* es un fenómeno ampliamente documentado en la literatura criminológica, que ocurre cuando los delincuentes modifican su conducta para evadir controles en lugar de desistir de la actividad ilícita. Puede manifestarse de diversas formas:

1. **Geográfico:** el delito se traslada a otra zona donde los controles son menores.
2. **Temporal:** se modifica el momento del ataque para evitar la vigilancia.
3. **De objetivo:** el infractor selecciona un blanco diferente menos protegido.
4. **De método:** se emplean técnicas o modalidades distintas para eludir controles.
5. **De tipo de crimen:** se sustituye una modalidad delictiva por otra más rentable o menos riesgosa.

Estudios de caso, como los realizados en el sector bancario y transporte de mercancías, muestran que la introducción de barreras físicas o tecnológicas puede reducir incidentes en un punto, pero incrementarlos en zonas adyacentes o mediante métodos alternativos (por ejemplo, fraude en línea tras reforzar la seguridad física). Para mitigar este fenómeno, se recomienda implementar análisis de impacto cruzado, monitoreo integral de incidentes y estrategias de prevención multifacéticas que no dejen brechas aprovechables por los infractores.

12.2 Adaptación tecnológica criminal

La adaptación tecnológica criminal se refiere a la capacidad de los infractores para identificar, estudiar y superar las barreras tecnológicas diseñadas para prevenir delitos. Esta tendencia se ha intensificado con la digitalización de procesos y la proliferación de dispositivos inteligentes (IoT), lo que ha generado nuevos retos para la seguridad patrimonial.

- Identificación de puntos ciegos en sistemas de videovigilancia mediante análisis de patrones de cobertura.
- Elusión de sensores o bloqueos electrónicos a través de técnicas de interferencia, clonación de señales o ataques de fuerza bruta.
- Uso de herramientas avanzadas, como malware, dispositivos de hardware modificados o exploits de vulnerabilidades para manipular sistemas.

Ejemplos recientes incluyen el bypass de alarmas inteligentes en automóviles mediante dispositivos OBD-II, el uso de ingeniería social para obtener accesos remotos y el fraude en cajeros automáticos (skimming). La respuesta efectiva requiere contramedidas como actualizaciones frecuentes de software, segmentación de redes, autenticación multifactor y capacitación continua del personal en nuevas amenazas.

12.3 Ataques contra sistemas de bloqueo

Los sistemas de bloqueo, ya sean físicos (candados, barreras mecánicas), electrónicos (firmware, servidores de autorización) o basados en IoT, son objetivos recurrentes de sabotaje, adulteración o intrusión. La naturaleza del riesgo radica en que, al ser puntos críticos de seguridad, su vulneración abre la puerta a pérdidas de alto impacto.

- Desactivación, manipulación o neutralización de mecanismos de seguridad usando herramientas especializadas.
- Explotación de vulnerabilidades en firmware, protocolos de comunicación inseguros o contramedidas mal implementadas.
- Uso de ataques combinados, integrando técnicas físicas y digitales para maximizar la probabilidad de éxito.

Para reducir estos riesgos, se recomienda realizar auditorías periódicas de seguridad (internas y por terceros), mantener actualizaciones constantes de firmware y software, practicar segmentación de redes, implementar pruebas de penetración y fortalecer la gestión de incidentes. El principio de defensa en profundidad y la redundancia de controles son fundamentos teóricos clave para robustecer la protección.

12.4 Escenarios de sabotaje interno

El sabotaje interno es uno de los riesgos más subestimados en la seguridad corporativa. Involucra a personas con acceso legítimo al sistema (empleados, contratistas, proveedores) que, por motivos de descontento, coacción, lucro o colusión con actores externos, pueden desactivar controles, manipular registros o facilitar accesos no autorizados.

- Desactivación deliberada de mecanismos de seguridad, como alarmas o registros de acceso.
- Falsificación o eliminación de registros de trazabilidad para ocultar actividades ilícitas.
- Compartición de credenciales o información sensible con grupos delictivos.

Ejemplos operativos incluyen la manipulación de inventarios en almacenes, la desactivación de sistemas de CCTV antes de un robo o el acceso indebido a bases de datos críticas. Para mitigar este riesgo, es fundamental aplicar controles de acceso basados en el principio de mínimo privilegio, monitorear actividades sospechosas, realizar rotación periódica de contraseñas y fomentar una cultura de denuncia y ética organizacional.

12.5 Estrategias de actualización continua

En un entorno donde tanto la tecnología como los métodos criminales evolucionan a gran velocidad, la gestión de riesgos efectiva exige actualizaciones y mejoras constantes en los controles y procesos. Esto se logra mediante:

1. **Revisión periódica de medidas existentes:** evaluar su eficacia frente a nuevas amenazas.
2. **Incorporación de inteligencia criminal:** analizar patrones emergentes, compartir información sectorial y anticipar tendencias.
3. **Evaluación de vulnerabilidades en tiempo real:** mediante monitoreo continuo, auditorías y pruebas de penetración.
4. **Capacitación constante del equipo de seguridad:** actualización en nuevas herramientas, técnicas y mejores prácticas.

Herramientas recomendadas incluyen equipos Red Team, escaneos automáticos de vulnerabilidades, benchmarking con la industria y suscripción a alertas de amenazas emergentes. El ciclo de mejora continua, basado en el modelo PDCA (Planificar-Hacer-Verificar-Actuar), garantiza la resiliencia y adaptación del sistema preventivo.

12.6 Simulación de escenarios adversos

La simulación de escenarios adversos es una práctica fundamental para anticipar la respuesta del sistema frente a ataques, evasiones o fallos inesperados. Permite identificar

debilidades antes de que sean explotadas y entrenar a los equipos de respuesta. Entre los tipos de simulaciones destacan:

- Modelos predictivos de desplazamiento del delito, basados en análisis estadístico y simuladores urbanos.
- Pruebas de resiliencia tecnológica ante ataques físicos, lógicos o combinados.
- Juegos de guerra (war-gaming) que simulan intrusiones internas, sabotaje o escenarios de crisis.
- Modelado de amenazas apoyado en datos históricos, inteligencia y patrones delictivos.

Para su aplicación práctica, se recomienda definir objetivos claros, involucrar a todas las áreas relevantes, documentar hallazgos y ajustar controles y protocolos en función de los resultados. Estas simulaciones deben formar parte del programa anual de gestión de riesgos y ser validadas por expertos externos para asegurar su objetividad.

Conclusión

La gestión de riesgos orientada a la prevención del delito exige un enfoque integral, proactivo y dinámico. Es indispensable analizar cómo los infractores pueden adaptarse y evolucionar ante los controles, considerando fenómenos como el desplazamiento del delito, la adaptación tecnológica, los ataques a sistemas de bloqueo y el sabotaje interno. Responder a estas amenazas requiere estrategias de actualización continua, simulación de escenarios adversos y la integración de mejores prácticas internacionales. Fortalecer el Modelo de Neutralización de Incentivo Delictivo (MNID) implica no solo proteger los activos presentes, sino anticipar y neutralizar las tácticas emergentes de criminalidad adaptativa, asegurando así la resiliencia y legitimidad de la gestión de riesgos corporativa.

Aplicación sectorial del Modelo de Neutralización de Incentivo Delictivo (MNID)

La gestión de riesgos delictivos exige un enfoque adaptado a la realidad de cada sector económico. El Modelo de Neutralización de Incentivo Delictivo (MNID) proporciona un marco robusto para anticipar, prevenir y responder a amenazas, pero su eficacia depende de la contextualización sectorial. Este análisis técnico aborda la aplicación del MNID en siete sectores clave, detallando riesgos, amenazas, estrategias, ejemplos y mejores prácticas internacionales, con el objetivo de fortalecer la resiliencia operativa y la legitimidad de la gestión corporativa.

13.1 Retail

Riesgos específicos: El sector retail enfrenta una gama de amenazas que incluyen hurtos en tienda, robos organizados (como “shop-steaming”), fraudes en puntos de venta

(POS), robo de identidad, robo de mercancía en almacenes y centros de distribución, y ataques a terminales de pago. Estos delitos impactan directamente en la rentabilidad y reputación de las cadenas comerciales, afectando tanto inventarios como la confianza del cliente.

Desarrollo detallado de amenazas: El shoplifting puede ser perpetrado por individuos o bandas especializadas, empleando técnicas de ocultamiento y distracción. El robo organizado, por ejemplo mediante grupos que saturan el personal de vigilancia, requiere respuestas integrales. Los fraudes en POS incluyen clonación de tarjetas y manipulación de terminales, lo que demanda soluciones tecnológicas y procesos de verificación robustos.

Aplicación ampliada del MNID:

- Desvalorización funcional: Marcaje permanente de mercancía de alto valor con etiquetas RFID, integración de sistemas de alarma y sensores de movimiento.
- Desvalorización comercial: Colaboración con bases de datos de bienes robados y plataformas de reporte, para que objetos “marcados” pierdan valor de reventa.
- Trazabilidad: Uso de IoT y cámaras con analítica inteligente para correlacionar eventos con inventario, permitiendo auditoría en tiempo real.
- Disuasión comunicacional: Señalización visible sobre monitoreo activo, bloqueos automáticos y consecuencias legales, reforzando la percepción de riesgo para los infractores.
- Sustitución del incentivo: Programas de recompra de productos fuera de cadena formal para desincentivar mercados paralelos.

Ejemplos y mejores prácticas internacionales: En Europa y Estados Unidos, la integración de sistemas RFID y la colaboración con fuerzas de seguridad han reducido el robo en tiendas hasta un 30%. El uso de “loss prevention teams” y la capacitación continua del personal son prácticas recomendadas. En México, la implementación de cámaras con analítica facial ha permitido identificar patrones de reincidencia.

13.2 Logística y transporte

Análisis de riesgos: El robo de carga en rutas y centros de distribución, extorsión y “derecho de piso”, sabotaje a rutas y equipos, y el robo de componentes de alto valor son amenazas recurrentes. Los delincuentes utilizan modus operandi sofisticados, como interceptación de GPS, falsificación de documentos y ataques coordinados en puntos vulnerables.

Estrategias avanzadas de neutralización:

- Desvalorización funcional: Implementación de bloqueos automáticos en equipos de transporte ante movimientos no autorizados, y marcaje de mercancías críticas que “caduquen” fuera de rutas autorizadas.

- Desvalorización comercial: Serialización de mercancías y partes para reducir la demanda en mercados ilegales.
- Trazabilidad: Sistemas IoT para monitoreo de ubicación, condición (temperatura, impacto) y estado de la carga, integrados con ERP y plataformas de control.
- Disuasión comunicacional: Señales visibles en vehículos y almacenes sobre monitoreo continuo, alertas automáticas y protocolos de respuesta rápida.
- Sustitución del incentivo: Alianzas entre transportistas para crear “entornos vigilados compartidos”, y programas de seguro vinculados a buenas prácticas de seguridad.

Casos de éxito y retos: El uso de telemática avanzada y “panic buttons” ha reducido el robo en rutas críticas. Sin embargo, la falta de colaboración intersectorial y la corrupción pueden limitar la efectividad. La integración de protocolos de respuesta conjunta con autoridades y la adopción de certificaciones internacionales (como TAPA) son claves para el éxito.

13.3 Tecnología y electrónicos

Amenazas físicas y cibernéticas: El sector tecnológico enfrenta robo de dispositivos físicos, robo de propiedad intelectual, fraude contra cadenas de suministro digitales, brechas de datos y filtración de información estratégica. Los incidentes pueden ser tanto internos (empleados) como externos (hackers, bandas organizadas).

Protección de propiedad intelectual e integración de ciberseguridad:

- Desvalorización funcional: Sistemas de bloqueo remoto y cifrado en dispositivos corporativos, dependencia de servidor para funciones clave.
- Desvalorización comercial: Serialización de hardware y certificación digital de software para que equipos “no autorizados” pierdan valor en reventa.
- Trazabilidad: Monitoreo integrado de activos físicos y licencias de software.
- Disuasión comunicacional: Mensajes visibles sobre seguridad de datos, cifrado y consecuencias legales.
- Sustitución del incentivo: Programas de recompra/actualización de equipos viejos para reducir mercado informal.

Ejemplos de incidentes y respuestas: El caso de ransomware WannaCry en 2017 demostró la importancia de segmentar redes y mantener actualizaciones de seguridad. Empresas mexicanas han implementado auditorías de activos y protocolos de respuesta ante incidentes, logrando reducir brechas de datos.

13.4 Energía e infraestructura crítica

Riesgos complejos: Las infraestructuras críticas (redes eléctricas, oleoductos, refinerías, telecomunicaciones) son objetivos de crimen común, ataques coordinados, sabotaje y

terrorismo. El impacto social y económico es elevado por la naturaleza esencial de los servicios.

Estrategias de defensa en profundidad:

- Desvalorización funcional: Segmentación de sistemas operativos críticos, control de acceso físico y digital.
- Desvalorización comercial: Registro y certificación de componentes para que su robo pierda valor si se extraen del entorno autorizado.
- Trazabilidad: IoT industrial y sistemas SCADA con detección de alteraciones en tiempo real.
- Disuasión comunicacional: Señales claras sobre monitoreo de instalaciones, vigilancia automática y respuesta coordinada con autoridades.
- Sustitución del incentivo: Programas que integran comunidades locales en protección de infraestructura y desarrollo socioeconómico.

Colaboración público-privada: La coordinación entre empresas, autoridades y comunidades es esencial. El ejemplo de la Comisión Federal de Electricidad (CFE) en México, que implementó sistemas de monitoreo remoto y programas sociales, ha reducido el sabotaje y robo de energía.

13.5 Sector farmacéutico

Delitos frecuentes: El sector farmacéutico enfrenta robo y hurto de medicamentos (especialmente controlados o de alto precio), falsificación y adulteración de productos, y acceso ilícito a salas de investigación. El impacto puede ser tanto económico como sanitario.

Trazabilidad avanzada y normativas regulatorias:

- Desvalorización funcional: Codificación y marcaje que invalida medicamentos fuera del ambiente controlado.
- Desvalorización comercial: Microdotting y tecnologías de identificación única para reducir valor de reventa.
- Trazabilidad: Sistemas avanzados de cadena de frío y blockchain para seguimiento de lote.
- Disuasión comunicacional: Comunicación de controles regulatorios estrictos y sanciones por comercialización ilegal.
- Sustitución del incentivo: Programas de devolución regulada de medicamentos caducos o sobrantes.

Experiencias internacionales: La Unión Europea exige serialización de todos los medicamentos, lo cual ha reducido la falsificación. En México, la COFEPRIS ha promovido la trazabilidad digital, aunque la falta de infraestructura limita la cobertura total.

13.6 Sector automotriz

Evolución de amenazas: El sector automotriz enfrenta robo de vehículos completos, robo de partes valiosas (airbags, catalizadores), clonación de llaves y ataques a software de vehículos conectados. Los delitos han evolucionado con la tecnología, incluyendo hackeo de sistemas de entrada sin llave.

Protección de vehículos conectados, serialización y trazabilidad:

- Desvalorización funcional: Sistemas de bloqueo remoto, cifrado de llaves y autenticación multifactor para iniciar el vehículo.
- Desvalorización comercial: Serialización de partes críticas y registro de propiedad para dificultar la reventa.
- Trazabilidad: GPS y telemática para seguimiento en tiempo real y alertas de anomalías.
- Disuasión comunicacional: Señales visibles sobre sistemas de seguridad activos.
- Sustitución del incentivo: Incentivos regulatorios para reciclaje y recompra de partes usadas.

Incentivos regulatorios y mejores prácticas: En Alemania, la obligatoriedad de sistemas antirrobo electrónicos ha reducido el robo de autos. En México, la colaboración entre fabricantes y aseguradoras para el registro de partes ha mejorado la trazabilidad.

13.7 Activos digitales

Amenazas emergentes: Los activos digitales incluyen datos, identidades digitales, credenciales y propiedad intelectual. Las amenazas van desde ransomware, phishing, robo de datos, ataques a infraestructura de nube y explotación de vulnerabilidades de software. El auge de lo digital ha convertido estos activos en blancos prioritarios de delincuentes cibernéticos.

Protección integral de datos, blockchain y auditoría:

- Desvalorización funcional: Cifrado de datos, autenticación fuerte y bloqueo automático tras intentos sospechosos.
- Desvalorización comercial: Hacer que los datos robados sean inútiles sin claves, empleando cifrado incomprometible.
- Trazabilidad: Logs inalterables y blockchain para auditoría inmutable de eventos.
- Disuasión comunicacional: Avisos de seguridad digital, sanciones legales y cooperación internacional (Convenio de Budapest).

- Sustitución del incentivo: Programas de formación digital que aumenten competencias legítimas y reduzcan participación en delitos digitales.

Formación y cultura de ciberseguridad: La capacitación continua, simulacros de respuesta y campañas de concientización son esenciales. Ejemplo: la implementación de "phishing drills" en bancos mexicanos ha reducido incidentes en un 40%.

Resumen

Cada sector presenta motivaciones y activos vulnerables distintos. La integración de medidas de desvalorización, trazabilidad, disuasión y sustitución de motivación, junto con la contextualización operativa, permite neutralizar incentivos delictivos de manera efectiva. El monitoreo continuo con indicadores específicos, la mejora permanente y la colaboración intersectorial son fundamentales para asegurar la resiliencia y legitimidad de la gestión de riesgos corporativa.

- Analiza *qué motiva* a los infractores en cada sector.
- Identifica *qué activos son más vulnerables*.
- Aplica medidas para *neutralizar el incentivo económico, funcional y operativo*.
- Integra acciones de *desvalorización, trazabilidad, disuasión y sustitución de motivación* según contexto.
- Monitorea continuamente con indicadores específicos por sector, ajustando estrategias ante nuevas amenazas.

Introducción: Importancia, Objetivos y Contexto de la Auditoría MNID

La auditoría del Modelo Nacional de Intervención y Desvalorización (MNID) representa una herramienta estratégica para la gestión de riesgos y la ciberseguridad corporativa. En un entorno donde la evolución de amenazas digitales es constante y la resiliencia organizacional depende de la capacidad de adaptación, el protocolo de auditoría MNID permite verificar, mejorar y certificar la eficacia de los controles implementados. Su objetivo es asegurar que el MNID no solo se ejecute conforme a lo planeado, sino que alcance niveles superiores de madurez, se adapte a nuevos riesgos y se integre con la gestión de riesgos de la organización.

Definición y Propósito del Protocolo de Auditoría MNID

Un protocolo de auditoría es un conjunto de pasos, criterios y mecanismos sistemáticos para evaluar, de manera objetiva, si el MNID está siendo implementado conforme a su diseño, cumple los objetivos planteados y genera los resultados esperados. Este protocolo trasciende la simple verificación: promueve el aprendizaje organizacional, la mejora continua y la alineación con la gestión de riesgos. Su valor estratégico radica en la capacidad de identificar desviaciones, descubrir oportunidades de mejora y fortalecer la legitimidad de los procesos corporativos.

Evaluación Inicial: Objetivos, Pasos, Herramientas y Buenas Prácticas

La evaluación inicial establece la línea de base para la auditoría MNID. Sus objetivos son:

- Determinar el estado actual del MNID antes del ciclo de auditoría.
- Identificar brechas entre la implementación real y el diseño esperado.
- Sentar las bases para comparaciones futuras y la evolución del sistema.

Pasos detallados:

1. **Definir alcance y criterios de auditoría:** Seleccionar los componentes a auditar (funcional, comercial, trazabilidad, disuasión, sustitución), determinar los documentos y procesos requeridos, y establecer indicadores clave.
2. **Recopilación de información inicial:** Reunir políticas, procedimientos, bases de datos de incidentes, reportes de riesgo y listas de controles implementados.
3. **Entrevistas preliminares:** Dialogar con responsables de cada componente para comprender la implementación práctica y detectar retos operativos.
4. **Mapeo preliminar de riesgos:** Identificar riesgos evidentes que puedan afectar la eficacia del MNID, utilizando matrices de riesgo, análisis de tendencias y revisión de incidentes previos.
5. **Documento de línea base:** Elaborar un reporte que resuma el estado inicial, las brechas identificadas y las prioridades de atención.

Herramientas recomendadas: Matrices de riesgo, listas de verificación, entrevistas estructuradas, análisis documental y paneles de indicadores sectoriales. Ejemplo de buena práctica: en auditorías de ciberseguridad bancaria, la línea base incluye una revisión exhaustiva de incidentes de “phishing” y controles asociados.

Verificación de Cumplimiento por Componente: Desarrollo Exhaustivo

La auditoría MNID debe desglosarse por cada uno de los cinco componentes, revisando evidencia de cumplimiento y operación. A continuación, se desarrolla cada componente con ejemplos de evidencias, métodos de verificación y casos prácticos:

1. **Desvalorización funcional:**
2. Revisar implementación de tecnologías de bloqueo remoto (ej. software de desactivación de equipos).
3. Comprobar protocolos de separación de posesión y funcionalidad, como autenticación multifactor.
4. Evaluar pruebas de resistencia, registros de activación/desactivación y simulacros de ataque.

5. *Ejemplo:* Empresas de manufactura utilizan sistemas IoT con bloqueo remoto ante robos; la auditoría verifica logs y capacidad de respuesta.
6. **Desvalorización comercial:**
7. Verificar marcajes de bienes y registros de serialización (etiquetas RFID, QR, etc.).
8. Revisar bases de datos públicas/internas para bienes marcados, y su consulta en operaciones.
9. Analizar reportes de mercado secundario: reducción de ventas ilegales tras marcaje.
10. *Ejemplo:* Auditoría en el sector automotriz revisa la trazabilidad de autopartes mediante serialización y bases de datos nacionales.
11. **Incremento de trazabilidad:**
12. Confirmar operación de sensores, sistemas IoT y plataformas de registro.
13. Validar integración con sistemas ERP y control interno.
14. Revisar alertas, logs de eventos y decisiones tomadas a partir de ellos.
15. *Ejemplo:* Auditoría en logística revisa sensores de rastreo y alertas automáticas ante desvíos de ruta.
16. **Disuasión comunicacional:**
17. Revisar señalizaciones, materiales de campaña y reportes de percepción de riesgo (encuestas, entrevistas).
18. Evaluar evidencia de comunicación interna y externa sobre mecanismos preventivos.
19. *Ejemplo:* Auditoría en universidades revisa campañas anti-phishing y la percepción de seguridad entre estudiantes.
20. **Sustitución del incentivo:**
21. Confirmar implementación de estrategias socialmente orientadas (programas de empleo, recompra, integración comunitaria).
22. Revisar indicadores estructurales (empleo, cohesión social) y su evolución.
23. *Ejemplo:* Auditoría a programas de reinserción laboral para exinfractores en sector tecnológico.

Estructura y Criterios de Auditoría: Objetividad, Normas Internacionales y Evidencia

Los criterios de auditoría deben ser objetivos, verificables y alineados con normas internacionales como ISO 19011 (Directrices para auditoría de sistemas de gestión) e ISO 27001 (Gestión de seguridad de la información). Se busca evidencia objetiva (documental,

registros, entrevistas) que demuestre que los procesos no solo existen, sino que **funcionan conforme a lo planeado**. Los criterios incluyen: definición de indicadores, documentación de procesos, registros de incidentes, y resultados de pruebas o simulacros.

Ejemplo de criterio: Para el componente de trazabilidad, la evidencia válida es la integración efectiva de sistemas de registro con alertas automatizadas y respuesta documentada ante incidentes.

Escala de Madurez MNID: Descripción, Indicadores y Uso para la Mejora

La **escala de madurez** permite calificar el nivel de implementación y efectividad del MNID en cada componente. Los niveles reflejan el grado de institucionalización, desde la informalidad hasta la optimización:

Nivel	Descripción	Indicadores Ejemplo
Inicial	Implementación parcial, procesos informales y evidencia mínima.	Documentos incompletos, controles ad hoc, poca trazabilidad.
Gestionado	Procesos definidos con algunos controles operativos en ejecución.	Procedimientos escritos, controles activos pero no sistemáticos.
Definido	Procedimientos documentados, consistentes y repetibles.	Auditoría periódica, registros completos, cumplimiento normativo.
Cuantitativamente gestionado	Medición formal de indicadores y toma de decisiones basada en datos.	Paneles de indicadores, análisis de tendencias, decisiones basadas en métricas.
Optimizado	Mejora continua, ajustes proactivos y adaptación a riesgos emergentes.	Innovación, automatización, adaptación ante amenazas nuevas.

Cada componente se califica de forma independiente, generando un perfil de madurez general y específico. La escala sirve como base para planificar mejoras y prioridades, y para comparar la evolución a lo largo del tiempo.

Modelos similares: CMMI, ISO 27001, marcos de auditoría de seguridad, donde los procesos evolucionan de ad hoc a optimizados.

Certificación Interna: Proceso, Actores, Beneficios y Relación con Auditorías Externas

La **certificación interna** valida que el MNID cumple criterios de calidad y eficacia definidos por la organización. No es una acreditación externa obligatoria, pero prepara al sistema para evaluaciones de terceros y fortalece la confianza interna.

Proceso:

1. Definición de criterios formales de aprobación, basados en evidencia recopilada y nivel mínimo de madurez.
2. Constitución de un comité de certificación imparcial que revisa resultados de auditoría.

3. Emisión de un certificado interno, indicando nivel de cumplimiento, alcance y fecha de revisión.
4. Periodo de validez, normalmente anual, con revisiones periódicas programadas.

Actores involucrados: Comité de certificación, responsables de cada componente, auditores internos, dirección corporativa.

Beneficios: Reconocimiento formal, establecimiento de estándares, motivación para alcanzar niveles superiores de madurez, preparación para auditorías externas (ISO 27001, etc.).

Ejemplo de certificado: Documento que especifica el nivel de madurez, componentes auditados, fecha de revisión y vigencia.

Plan de Mejora Continua: Componentes, Metodología, Ejemplos y Relación con Gestión de Riesgos

El objetivo final de la auditoría es **generar acciones de mejora continua**. Este proceso asegura que el MNID evolucione ante cambios del entorno o nuevas amenazas, integrándose con la gestión de riesgos (ISO 31000).

Componentes del plan de mejora:

1. Registro de hallazgos y no conformidades, con responsable y prioridad asignada.
2. Acciones correctivas y preventivas, orientadas a eliminar causas raíz y evitar recurrencias.
3. Objetivos de mejora concretos, con metas a corto, mediano y largo plazo e indicadores asociados.
4. Cronograma y recursos asignados, detallando fechas de cumplimiento y presupuestos requeridos.
5. Seguimiento y evaluación de resultados, mediante revisión periódica de avances contra indicadores.

Metodología recomendada: Ciclo PDCA (Plan-Do-Check-Act), revisiones periódicas, integración de resultados de auditoría, retroalimentación de responsables.

Ejemplo: Tras detectar una brecha en trazabilidad, se implementan sensores adicionales y se revisan protocolos de respuesta; el avance se mide con indicadores de reducción de incidentes.

Relación con gestión de riesgos: El plan de mejora se integra con la gestión de riesgos dinámica, asegurando que la organización responda adecuadamente a cambios internos y externos, conforme a ISO 31000.

Resumen

El protocolo de auditoría MNID es una herramienta clave para asegurar que los sistemas de intervención y desvalorización no solo existen, sino que funcionan, evolucionan y se adaptan a nuevos riesgos. Su implementación debe ser rigurosa, basada en criterios objetivos, evidencia verificable y alineada con mejores prácticas internacionales. Se recomienda:

- Integrar la auditoría MNID con la gestión de riesgos corporativa.
- Utilizar la escala de madurez para planificar mejoras y medir evolución.
- Fomentar la certificación interna como preparación para auditorías externas.
- Implementar planes de mejora continua que aseguren adaptación y resiliencia ante amenazas emergentes.

Una auditoría bien diseñada y ejecutada convierte el MNID en un motor de cambio y legitimidad, fortaleciendo la resiliencia y efectividad de la organización en el entorno digital actual.

15. CONCLUSIONES ESTRATÉGICAS

Las conclusiones estratégicas sintetizan los principales aprendizajes de todo el Manual Modelo de Neutralización de Incentivo Delictivo (MNID) y articulan qué significa este modelo para la seguridad organizacional, la prevención del delito y el desarrollo de enfoques sistémicos de gestión de riesgo. Se trata de traducir teoría en impacto, y de posicionar el MNID como una herramienta no solo operativa, sino transformadora.

15.1 Transformación del enfoque de seguridad

La seguridad contemporánea ya no es únicamente reactiva ni punitiva. Tradicionalmente se respondía al delito después de que ocurriera —mediante castigos, investigaciones o sanciones—, pero la evidencia criminológica y de políticas públicas apunta a que este enfoque aislado:

- No altera las causas profundas del delito.
- Suele generar ciclos de criminalidad persistentes.
- No es sostenible en recursos.

Un cambio estratégico moderno, que el MNID incorpora, es mover la seguridad hacia un enfoque preventivo, sistémico y basado en gestión de riesgo, donde se actúa *antes* de que ocurra el delito y *en los incentivos* que lo motivan. Esto está alineado con prácticas como la prevención situacional del delito (enfocada en condiciones que facilitan los delitos) y la prevención social (centrada en factores estructurales y comunitarios) ambas ampliamente respaldadas por la criminología contemporánea.

Este modelo transforma el enfoque de seguridad de:

- Reacción a hechos consumados
- Prevención integral, orientada a riesgo e incentivos

Así se amplía el campo de acción de la seguridad hacia la gestión proactiva del contexto, la percepción y las consecuencias.

15.2 Neutralización vs confrontación

Tradicionalmente la seguridad gravitaba alrededor de dos grandes estrategias:

1. **Confrontación directa**: perseguir, sancionar y penalizar al infractor (enfoque penal y policial clásico).
2. **Defensa reactiva**: reforzar barreras y vigilancia tras incidentes.

Ambos enfoques se ubican en la lógica de *disuasión por castigo*, que puede tener efecto, pero no siempre modifica la ecuación de decisión del actor delictivo, y en ocasiones puede generar efectos adversos como desplazamiento del delito o sobreconcentración de recursos en medidas simbólicas sin impacto real de largo plazo.

El MNID propone, en cambio, una neutralización de incentivos:

- **Modificar el valor percibido del delito** para el infractor.
- **Reducir la utilidad real del bien sustraído** (desvalorización funcional y comercial).
- **Incrementar riesgos y costos calculados** asociados a la conducta delictiva.
- **Atacar las causas estructurales que generan motivación delictiva.**

Esta perspectiva no es **antagónica** a la confrontación, sino complementaria: disminuye la necesidad de confrontar porque reduce la probabilidad de que ocurra el evento. Así, se prioriza:

➞ menor *oportunidad*
➞ menor *beneficio percibido*
➞ mayor *percepción de riesgo*

—y no solo mayor *castigo*.

15.3 Impacto sistémico a mediano y largo plazo

Un enfoque como el MNID puede generar impactos más profundos y sostenibles que las medidas aisladas de seguridad. Este impacto se materializa en varias dimensiones:

Dimensión operativa

- Menor frecuencia de delitos específicos contra activos críticos.
- Mayor recuperación de bienes sustraídos gracias a trazabilidad.

- Reducción de pérdidas económicas por delitos patrimoniales.

Dimensión conductual

- Cambios en la percepción de riesgo y beneficio de los infractores potenciales.
- Reducción de intento delictivo incluso en presencia de oportunidades.
  Esto se logra porque el modelo actúa sobre la percepción, que en criminología es clave para la toma de decisiones delictivas.

Dimensión social y estructural

- Incremento en el capital social y cohesión comunitaria.
- Disminución de factores socioeconómicos que presionan a conductas delictivas.
- Fortalecimiento de cultura preventiva dentro y fuera de la organización.

Dimensión estratégica

- Un enfoque integrado como el MNID genera una gestión sistémica de seguridad en lugar de fragmentada.
- Permite analizar y responder a riesgos emergentes antes de que se conviertan en crisis.

Este impacto sistémico no es inmediato, sino acumulativo y escalable: las acciones preventivas generan externalidades positivas que se refuerzan con el tiempo, haciendo que la reducción del delito se sostenga más allá de un periodo puntual.

15.4 Recomendaciones para expansión sectorial

Para que el MNID no se limite a implementaciones aisladas o sectoriales, sino que se convierta en un enfoque ampliable, adaptable y sostenible, se recomienda:

1. Adaptación contextual

Cada sector —retail, logística, energía, farmacéutico, automotriz, activos digitales, infraestructura crítica— tiene patrones de riesgo distintos. Por ello, el MNID debe traducirse en protocolos sectoriales específicos, con indicadores y mecanismos propios adaptados al contexto operativo y regulatorio.

2. Cooperación interinstitucional

La seguridad sistémica requiere colaboración entre actores públicos, privados, académicos y comunitarios. La gobernanza de seguridad contemporánea depende de redes colaborativas y corresponsabilidad amplia, no solo de jurisdicciones cerradas.

3. Integración de ciencia e inteligencia criminológica

Incorporar análisis sistemático, modelización de tendencias delictivas y evaluación continua de evidencia permite que las decisiones estratégicas no dependan solo de intuiciones o normas rígidas, sino de información real y actualizada. Estudios criminológicos han mostrado que estrategias basadas en evidencia pueden reducir delitos de forma significativa cuando están bien implementadas.

4. Monitoreo y mejora continua

Los riesgos —especialmente tecnológicos y sociales— evolucionan rápidamente. Por ello, los programas sectoriales deben incluir ciclos de auditoría, evaluación y actualización **continua** para adaptarse a nuevas amenazas y comportamientos delictivos emergentes, tanto físicos como digitales.

5. Énfasis en cultura preventiva

Fomentar una cultura preventiva dentro de organizaciones y comunidades donde la seguridad no es vista como un costo, sino como un valor estratégico contribuirá a internalizar prácticas de neutralización de incentivo en la rutina y operaciones cotidianas.

Síntesis

El MNID representa una evolución del enfoque de seguridad, orientada a gestionar incentivos, oportunidades y percepciones antes de que un delito ocurra, en lugar de sólo responder después. Este cambio no solo integra metodologías contemporáneas de prevención del delito, sino que se alinea con mejores prácticas de gestión de riesgo, criminología y políticas públicas, creando un marco sistémico, adaptable, mensurable y sostenible en cualquier sector.

Referencias

Clarke, R. V. (1997). *Situational crime prevention: Successful case studies* (2nd ed.). Harrow and Heston.

Clarke, R. V., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. *Crime and Justice, 6*, 147–185. https://doi.org/10.1086/449106

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies, 16*, 41–96.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://doi.org/10.2307/2094589

Felson, M., & Clarke, R. V. (1998). *Opportunity makes the thief: Practical theory for crime prevention*. Home Office, Policing and Reducing Crime Unit.

United Nations Office on Drugs and Crime (UNODC). (2010). *Handbook on the crime prevention guidelines: Making them work*. United Nations.

United Nations Office on Drugs and Crime (UNODC). (2019). *Education for Justice (E4J) University Module Series: Crime Prevention*. United Nations.

International Organization for Standardization (ISO). (2018). *ISO 19011:2018 – Guidelines for auditing management systems*. ISO.

International Organization for Standardization (ISO). (2018). *ISO 31000:2018 – Risk management — Guidelines*. ISO.

International Organization for Standardization (ISO). (2022). *ISO/IEC 27001:2022 – Information security management systems — Requirements*. ISO.

National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*. U.S. Department of Commerce.

National Institute of Standards and Technology (NIST). (2020). *Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5)*. U.S. Department of Commerce.

European Union Agency for Cybersecurity (ENISA). (2022). *Threat Landscape Report*. ENISA.

Organisation for Economic Co-operation and Development (OECD). (2020). *Reducing the risk of wholesale financial crime: Improving data sharing and analysis*. OECD Publishing.

Beccaria, C. (1764/1986). *On crimes and punishments*. Hackett Publishing.

World Bank. (2011). *Crime and violence in Central America: A development challenge*. World Bank.

CMMI Institute. (2018). *CMMI for Development, Version 2.0*. ISACA.

Kaplan, R. S., & Norton, D. P. (1996). *The balanced scorecard: Translating strategy into action*. Harvard Business School Press.

Porter, M. E. (1985). *Competitive advantage: Creating and sustaining superior perfor*

mance. Free Press.